ciso
Carnegie Mellon University

Operational Resilience

Dr. Nader Mehravari, MBCP, MBCI

Cyber Risk and Resilience Management Team
Software Engineering Institute
Carnegie Mellon University
nmehravari@sei.cmu.edu
http://www.cert.org/resilience/

October 16, 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **16 OCT 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Operational Resilience**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Dr. Nader Mehravari**	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Cyber Risk and Resilience Management Team Software Engineering Institute Carnegie Mellon University**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**262**	

Outline of the Session

Setting the Stage	• Three Stories; Same Conclusion.	**Guidance for Putting it into Practice**
Organizational Mission	• Why are we having this discussion?	
Operational Stress	• A look at recent events	
Yesterday vs. Today	• What has changed?	
Operational Resilience	• Risk and Resilience • Concepts of Resilience and Operational Resilience • Cornerstones of Operational Resilience	
Maturity Models	• ABCs of Maturity Models	
Overview of CERT-RMM	• Background and History • Organization of the Model • Using the Model • Distinguishing Features of CERT-RMM	
Success Stores	• DHS (CRR) • DOE (ES-C2M2) • USPS • Lockheed Martin	
Challenges	• Unsolved problems	
Summary	• A few key reminders	

NOTE: Guidance for Putting it into Practice

Two sample (very different) scenarios for putting principles of operational resilience into practice:

1. After a major and visible disruptive event has taken place and you want to apply concepts from his module to deal with it.

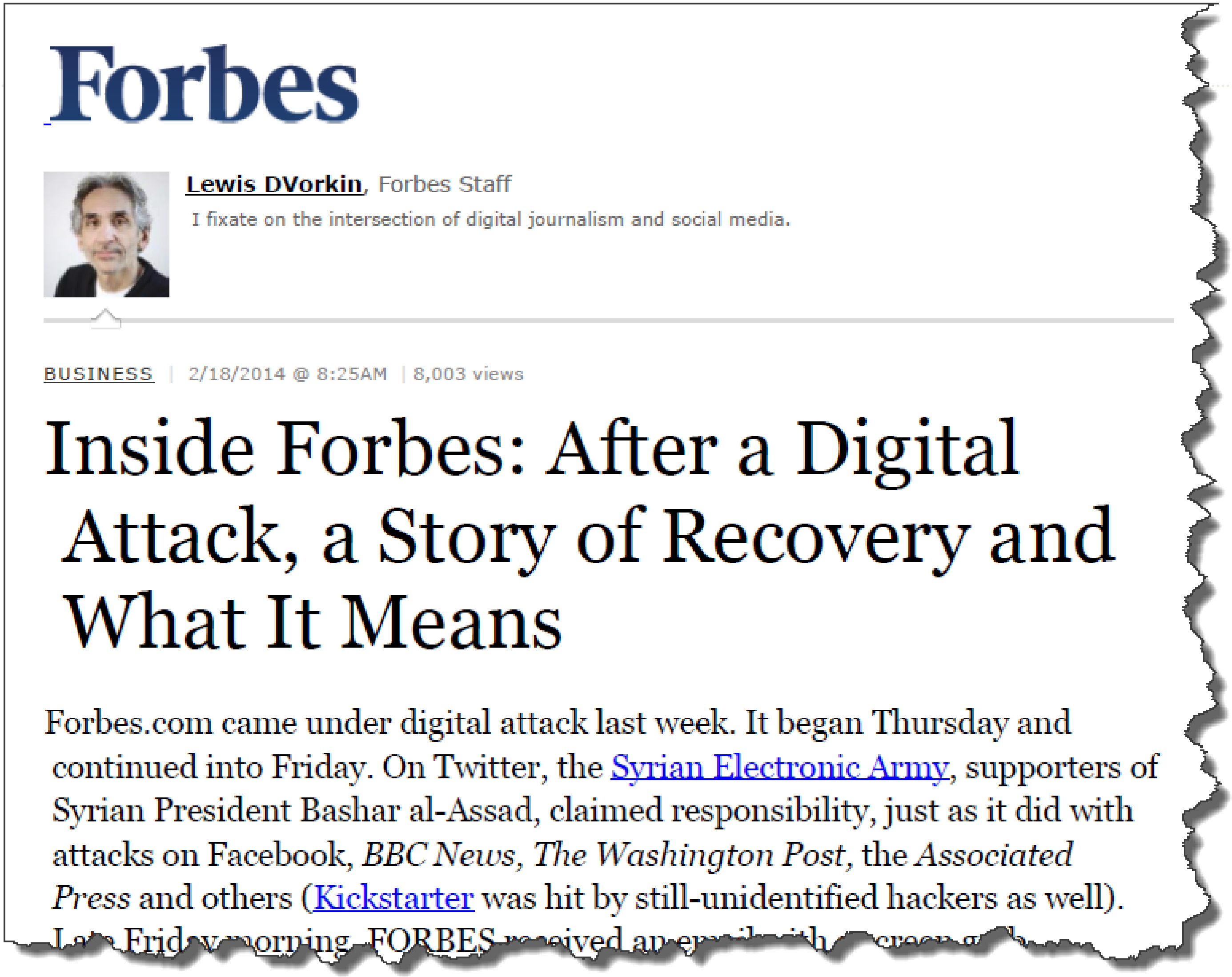
2. The there is a (business) desire to put in place a strategic plan and program to raise the bar.

Setting the Stage

Three Stories; Same Conclusion.

February 2014 Hacking of Forbes, Inc.

(Phishing is popular and effective)
(Some people will never change)



Forbes

Lewis DVorkin, Forbes Staff

I fixate on the intersection of digital journalism and social media.

BUSINESS | 2/18/2014 @ 8:25AM | 8,003 views

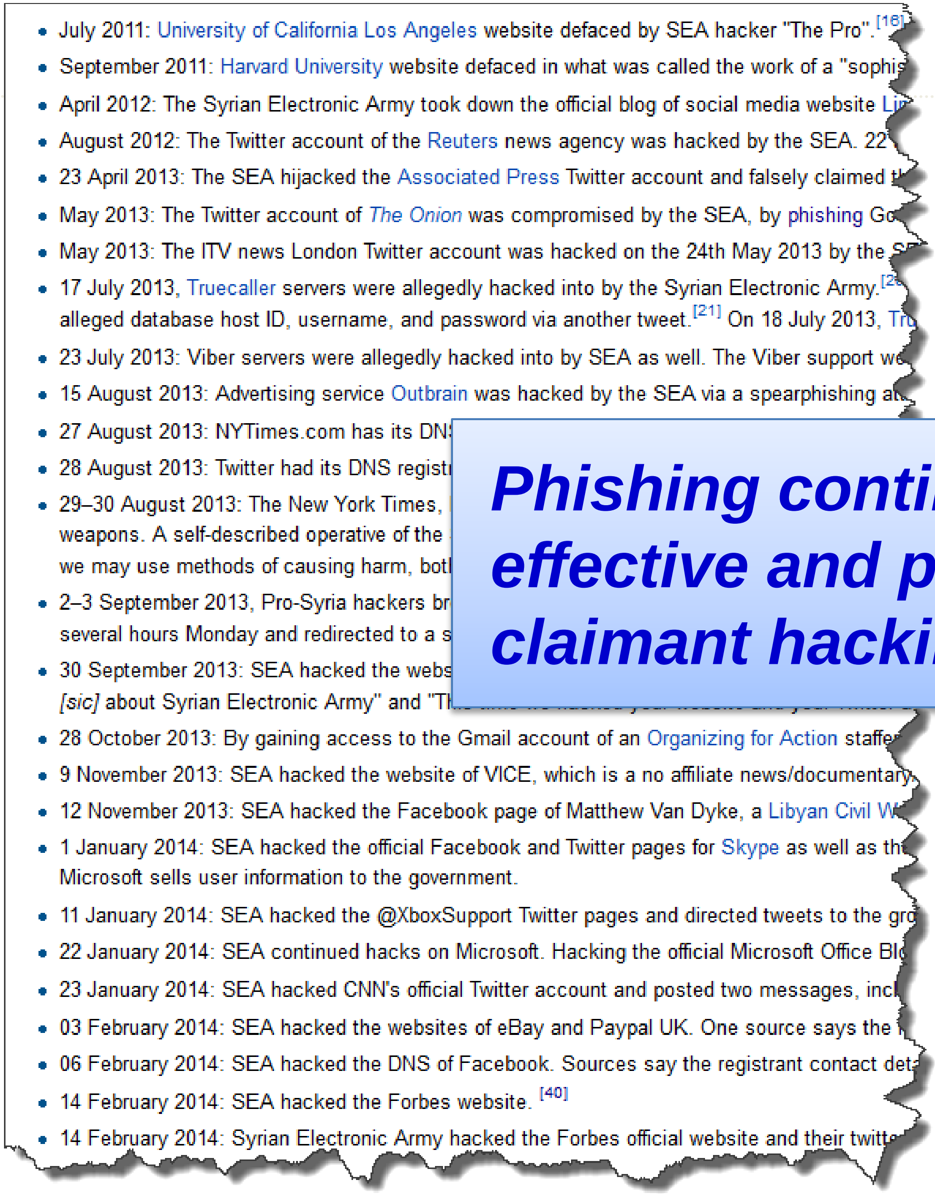
Inside Forbes: After a Digital Attack, a Story of Recovery and What It Means

Forbes.com came under digital attack last week. It began Thursday and continued into Friday. On Twitter, the Syrian Electronic Army, supporters of Syrian President Bashar al-Assad, claimed responsibility, just as it did with attacks on Facebook, *BBC News, The Washington Post*, the *Associated Press* and others (Kickstarter was hit by still-unidentified hackers as well). Late Friday morning, FORBES received an email with a screen gr

"…We could have done real damage but we restrained ourselves… We only published the database for one day… We were able to delete everything but we didn't: the files, the articles, the whole database…"

Claimant hacking organization's representative

2011



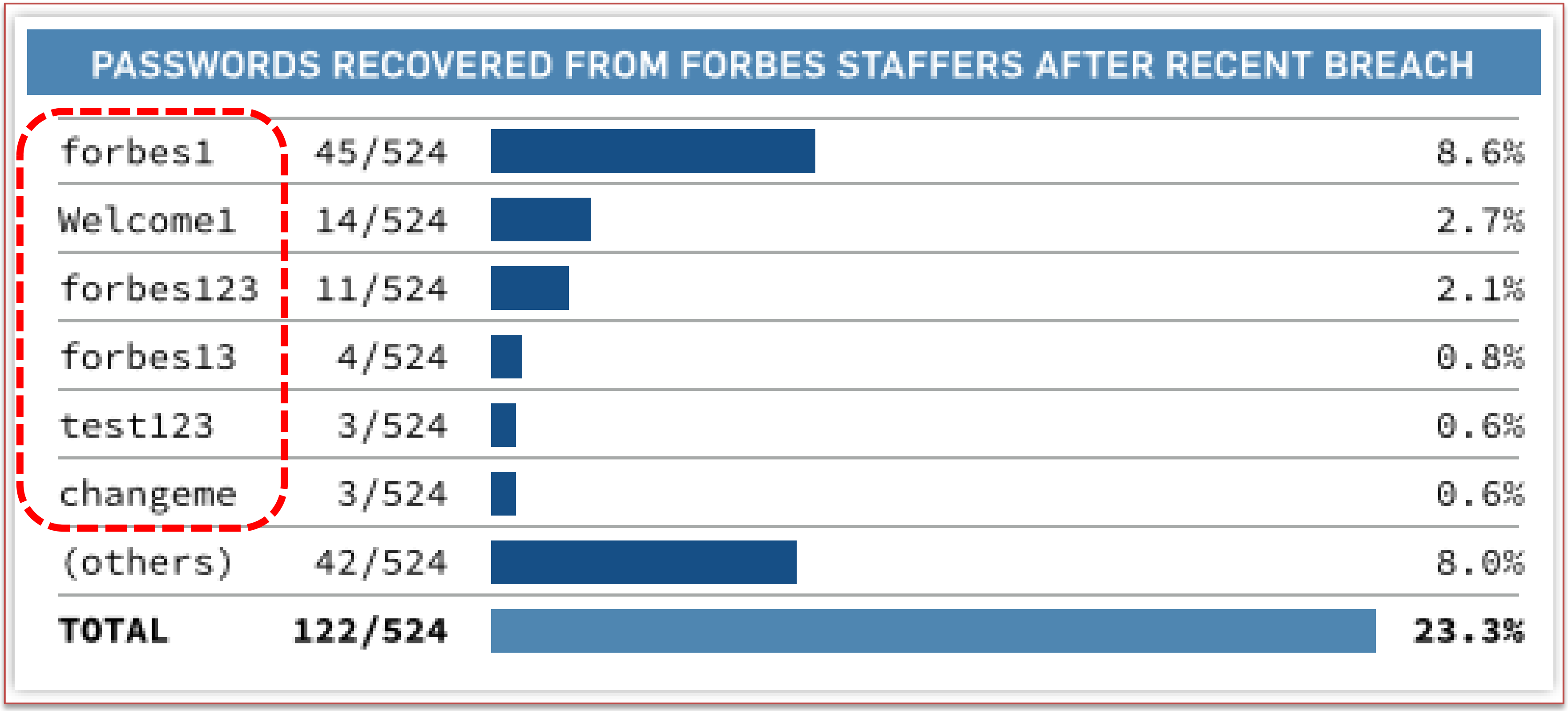
- July 2011: University of California Los Angeles website defaced by SEA hacker "The Pro".[16]
- September 2011: Harvard University website defaced in what was called the work of a "sophis
- April 2012: The Syrian Electronic Army took down the official blog of social media website Li
- August 2012: The Twitter account of the Reuters news agency was hacked by the SEA. 22
- 23 April 2013: The SEA hijacked the Associated Press Twitter account and falsely claimed t
- May 2013: The Twitter account of *The Onion* was compromised by the SEA, by phishing Go
- May 2013: The ITV news London Twitter account was hacked on the 24th May 2013 by the S
- 17 July 2013, Truecaller servers were allegedly hacked into by the Syrian Electronic Army.[2 alleged database host ID, username, and password via another tweet.[21] On 18 July 2013, Tr
- 23 July 2013: Viber servers were allegedly hacked into by SEA as well. The Viber support we
- 15 August 2013: Advertising service Outbrain was hacked by the SEA via a spearphishing at
- 27 August 2013: NYTimes.com has its DN
- 28 August 2013: Twitter had its DNS regist
- 29–30 August 2013: The New York Times, weapons. A self-described operative of the we may use methods of causing harm, bot
- 2–3 September 2013, Pro-Syria hackers br several hours Monday and redirected to a s
- 30 September 2013: SEA hacked the webs *[sic]* about Syrian Electronic Army" and "T
- 28 October 2013: By gaining access to the Gmail account of an Organizing for Action staffe
- 9 November 2013: SEA hacked the website of VICE, which is a no affiliate news/documentary
- 12 November 2013: SEA hacked the Facebook page of Matthew Van Dyke, a Libyan Civil W
- 1 January 2014: SEA hacked the official Facebook and Twitter pages for Skype as well as th Microsoft sells user information to the government.
- 11 January 2014: SEA hacked the @XboxSupport Twitter pages and directed tweets to the gro
- 22 January 2014: SEA continued hacks on Microsoft. Hacking the official Microsoft Office Bl
- 23 January 2014: SEA hacked CNN's official Twitter account and posted two messages, inc
- 03 February 2014: SEA hacked the websites of eBay and Paypal UK. One source says the
- 06 February 2014: SEA hacked the DNS of Facebook. Sources say the registrant contact det
- 14 February 2014: SEA hacked the Forbes website. [40]
- 14 February 2014: Syrian Electronic Army hacked the Forbes official website and their twitt

2014

Phishing continues to be effective and popular with the claimant hacking organization

http://en.wikipedia.org/wiki/Syrian_Electronic_Army

Some people will never change



PASSWORDS RECOVERED FROM FORBES STAFFERS AFTER RECENT BREACH

forbes1	45/524	8.6%
Welcome1	14/524	2.7%
forbes123	11/524	2.1%
forbes13	4/524	0.8%
test123	3/524	0.6%
changeme	3/524	0.6%
(others)	42/524	8.0%
TOTAL	**122/524**	**23.3%**

http://nakedsecurity.sophos.com/2014/02/17/forbes-hack-password-shootout-gmail-vs-yahoo-vs-hotmail-vs-aol-whose-users-are-the-smartest/

Environment that Forbes Operates In

"…There are challenges and risks associated with a platform that supports a distributed workforce using a distributed set of tools in a social news environment…"

"…Certain consumer friendly features, such as social log-ons and plug-ins that enhance the news product, carry their own vulnerabilities. The rewards of innovation are significant…"

Lewis Dvorkin
Chief Product Officer of Forbes Media

Sandy's Surprises

Hurricane Sandy – Basic Statistics

Developed	October 22, 2012
Dissipated	October 31, 2012
Highest winds	115 mph
Lowest pressure	940 mbar
Strength	Category 3 hurricane at its peak intensity
Size	Winds spanning 1,100 miles
Power Outages	Peaked at 8.2 million customers (October 30)
Fatalities	147 direct (138 indirect)
Economic damage	Estimated to be $75 billion
Nicknames	Superstorm Sandy; Frankenstrom

Hurricane Sandy – Affected Regions

Caribbean

- Jamaica
- Haiti
- Bahamas
- Bermuda
- Cuba

United States

- Florida
- North & South Carolina
- West Virginia
- Virginia
- Maryland
- Delaware
- New Jersey
- New York
- Pennsylvania
- New England region
- Great Lakes region
- Appalachian Mountains region

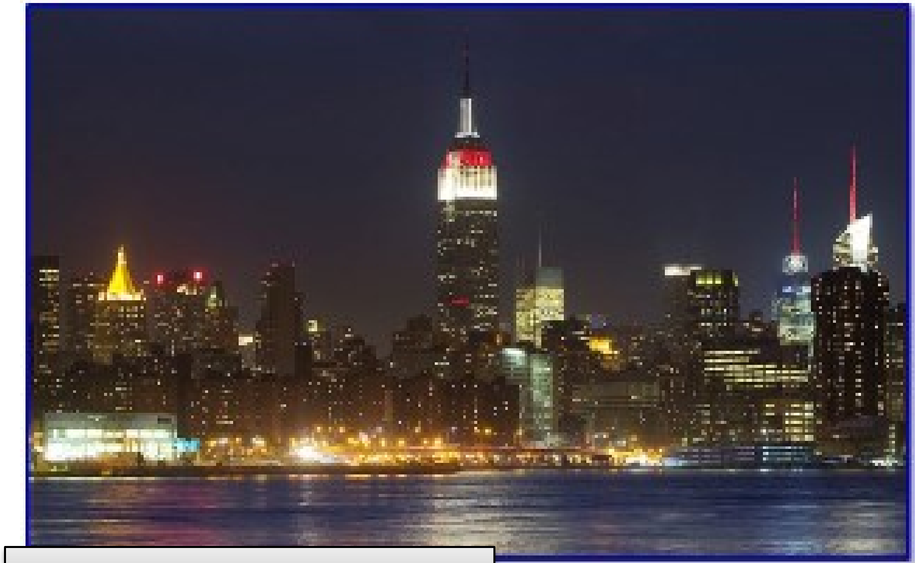
Canada

Quebec City
Ottawa
Montreal
Maine
Vermont
Michigan
Toronto
New Hampshire
New York
Detroit
Massachusetts
Chicago
Connecticut
Rhode Island
Pennsylvania
New York
Ohio
Indiana
Philadelphia
Columbus
Indianapolis
Maryland
New Jersey
West Virginia
Delaware
District of Columbia
Kentucky
Virginia
Tennessee
North Carolina
Charlotte
Atlanta
South Carolina
Alabama
Georgia
Jacksonville
Tampa
Florida
Miami
The Bahamas
Cape Coral
Freeport
Fort Lauderdale
Miami
Everglades National Park
Nassau
The Bahamas
Havana
Matanzas
Pinar del Rio
Artemisa
Colón
Santa Clara
Cienfuegos
Cuba
Puerto Padre
Camaguey
Las Tunas
Holguin
Bayamo
Guantanamo
Santiago de Cuba
Turks and Caicos Islands
Cap-Haitien
Gonaives
Santiago De Los Caballeros
Cayman Islands
Haiti
Dominican Republic
Montego Bay
Port-au-Prince
La Romana
Jamaica
Jacmel
Hayes

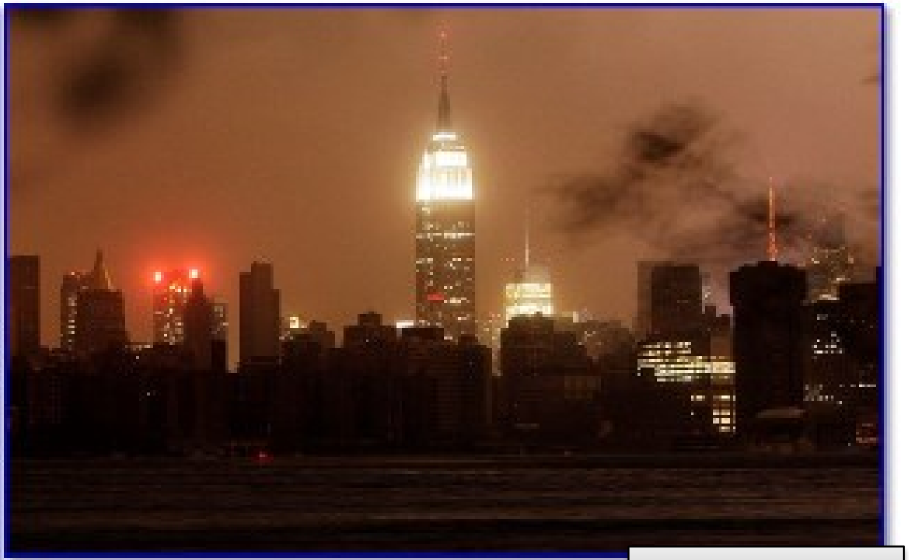
Large hurricane but expected… Flooding

Large but expected… Wind Damage

Large but expected… Loss of Power



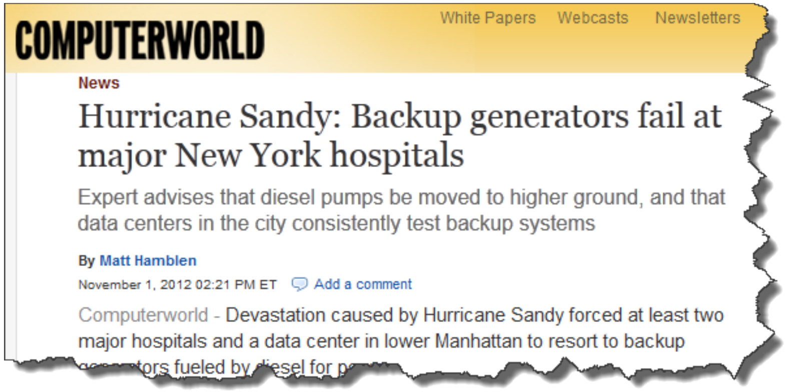
Typical Manhattan evening view



October 29, 2012

Large but expected… Demand for generators

Unexpected – Failures of numerous…



COMPUTERWORLD White Papers Webcasts Newsletters

News

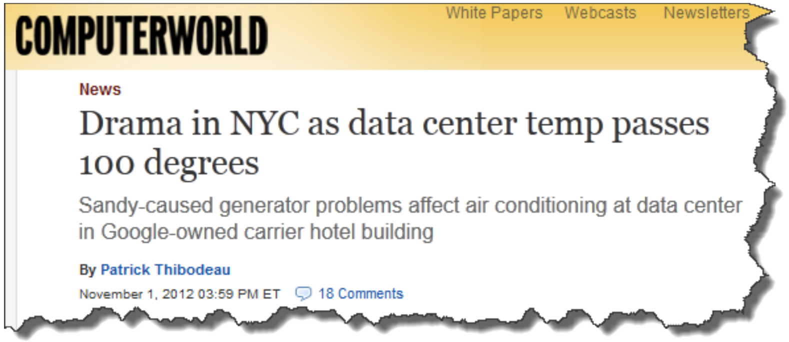
Hurricane Sandy: Backup generators fail at major New York hospitals

Expert advises that diesel pumps be moved to higher ground, and that data centers in the city consistently test backup systems

By Matt Hamblen

November 1, 2012 02:21 PM ET Add a comment

Computerworld - Devastation caused by Hurricane Sandy forced at least two major hospitals and a data center in lower Manhattan to resort to backup generators fueled by diesel for p



COMPUTERWORLD White Papers Webcasts Newsletters

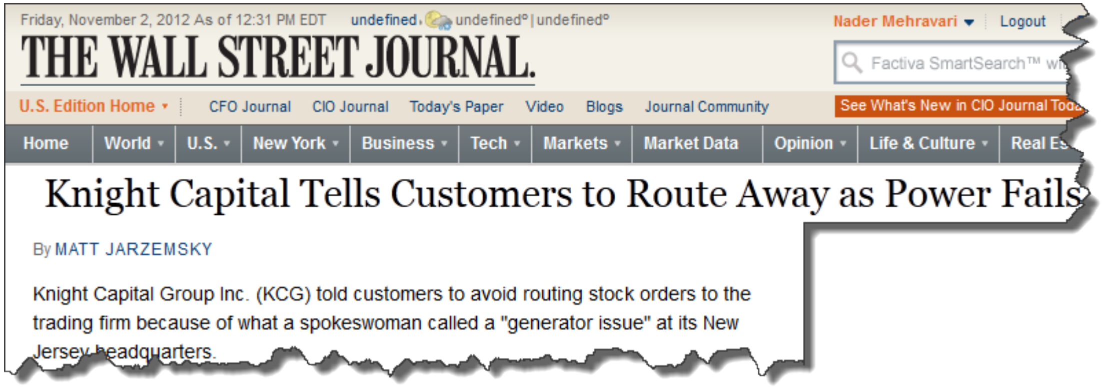
News

Drama in NYC as data center temp passes 100 degrees

Sandy-caused generator problems affect air conditioning at data center in Google-owned carrier hotel building

By Patrick Thibodeau

November 1, 2012 03:59 PM ET 18 Comments



Friday, November 2, 2012 As of 12:31 PM EDT undefined, undefined° | undefined° Nader Mehravari Logout

THE WALL STREET JOURNAL.

Factiva SmartSearch™ wi

U.S. Edition Home CFO Journal CIO Journal Today's Paper Video Blogs Journal Community See What's New in CIO Journal Tod

Home World U.S. New York Business Tech Markets Market Data Opinion Life & Culture Real Es

Knight Capital Tells Customers to Route Away as Power Fails

By MATT JARZEMSKY

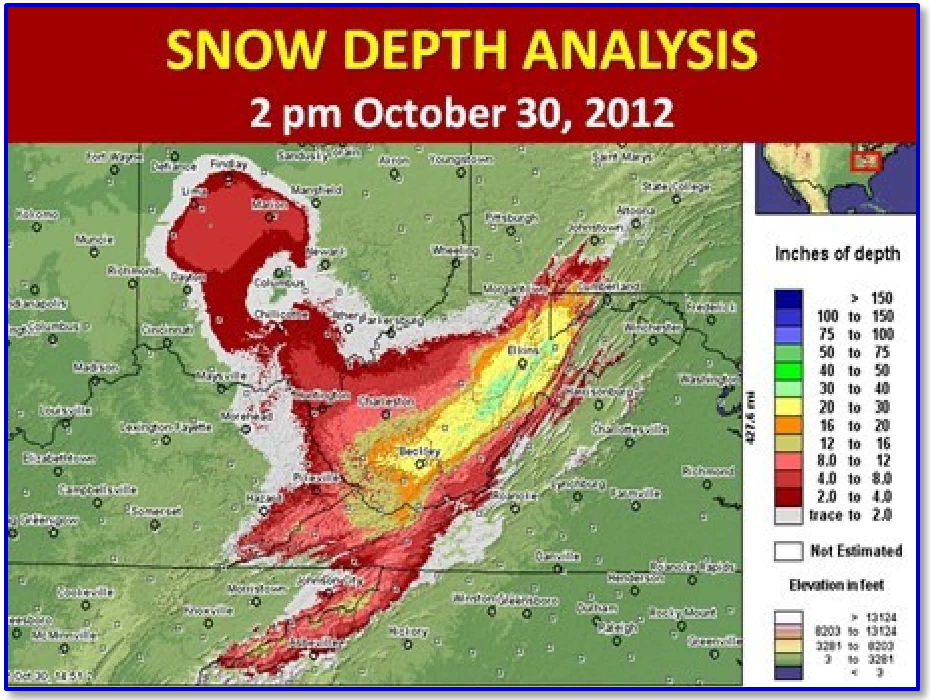
Knight Capital Group Inc. (KCG) told customers to avoid routing stock orders to the trading firm because of what a spokeswoman called a "generator issue" at its New Jersey headquarters.

… backup generators in hospitals and data centers

Unexpected - Major Devastating Fire

Breezy Point neighborhood, Queens, NY

Unexpected – Blizzard


SNOW DEPTH ANALYSIS

2 pm October 30, 2012

West Virginia

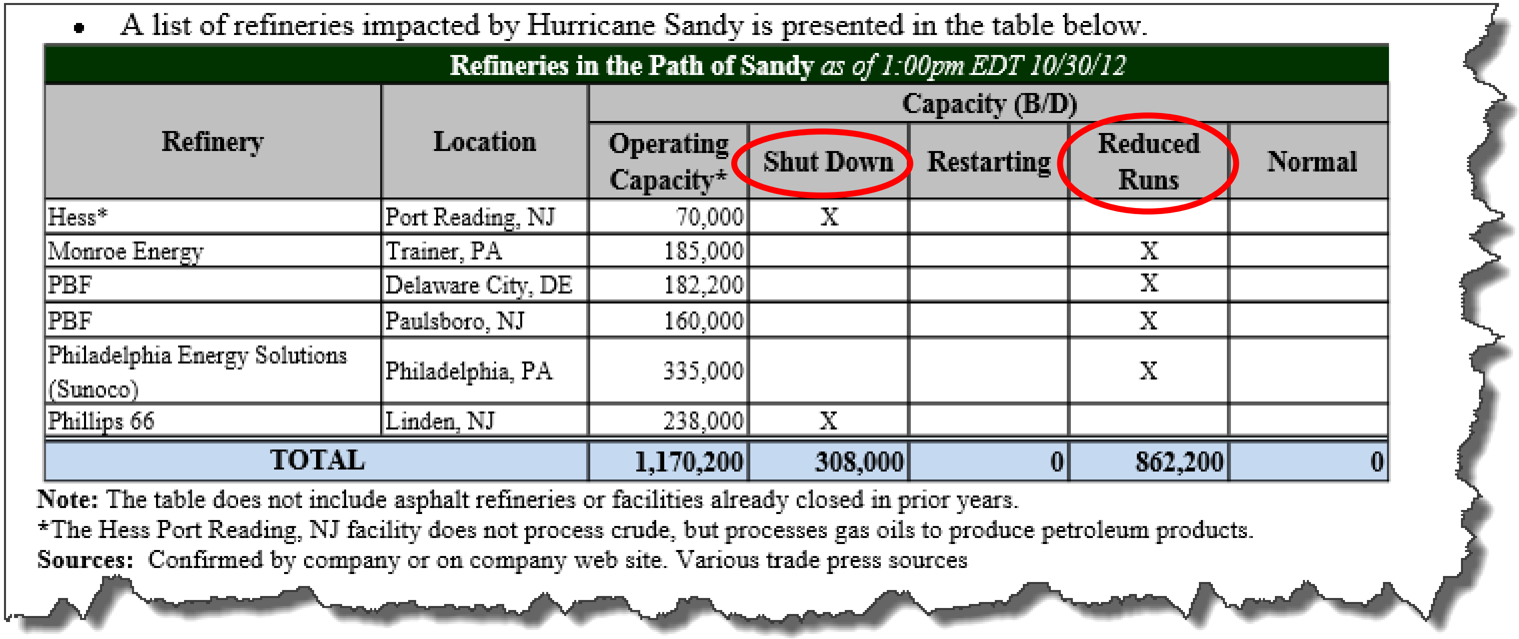
Unexpected – Acting like a sandstorm

Seaside Heights, NJ - Before

Cape May, NJ - After

Seaside Heights, NJ - After

Unexpected – Petroleum Shortage



- A list of refineries impacted by Hurricane Sandy is presented in the table below.

Refineries in the Path of Sandy *as of 1:00pm EDT 10/30/12*

Refinery	Location	Capacity (B/D)				
		Operating Capacity*	Shut Down	Restarting	Reduced Runs	Normal
Hess*	Port Reading, NJ	70,000	X			
Monroe Energy	Trainer, PA	185,000			X	
PBF	Delaware City, DE	182,200			X	
PBF	Paulsboro, NJ	160,000			X	
Philadelphia Energy Solutions (Sunoco)	Philadelphia, PA	335,000			X	
Phillips 66	Linden, NJ	238,000	X			
TOTAL		**1,170,200**	**308,000**	**0**	**862,200**	**0**

Note: The table does not include asphalt refineries or facilities already closed in prior years.
*The Hess Port Reading, NJ facility does not process crude, but processes gas oils to produce petroleum products.
Sources: Confirmed by company or on company web site. Various trade press sources

Unexpected – Run on…

ATM Vestibule

Shelter

CNN Mobile Unit

…power strips

Disruptive events, through which risks are realized, will continue to surprise us.

Traditional tools, techniques, and methods may not work as well in this environment.

Nader’s Briefcase

Changes Since 9/11

September 11, 2001

I was on a business trip out of town.

My briefcase contained

- **A laptop**
- **An analog cell phone**

September 11, 2014

I was on a business trip out of town.

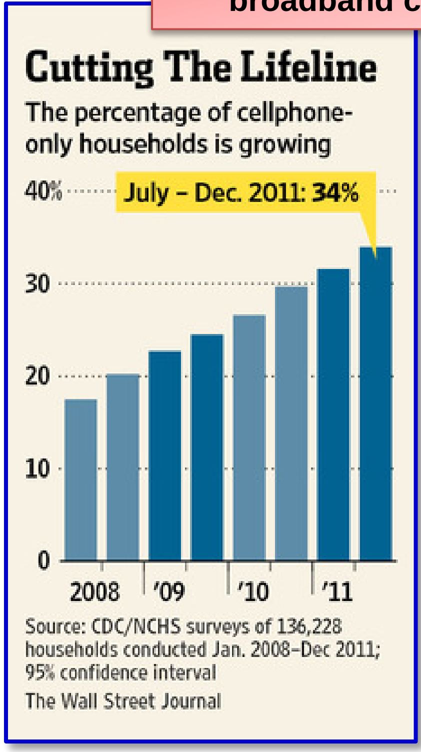
My briefcase contained

- **11 devices needing frequent charging**
- **Majority with some form of wireless capability**

Expanding and Dynamic Risk Environment

How has the critical infrastructure risk environment changed since 9/11:

Movement from traditional wireline telephony to cell phones and broadband cable telephony.

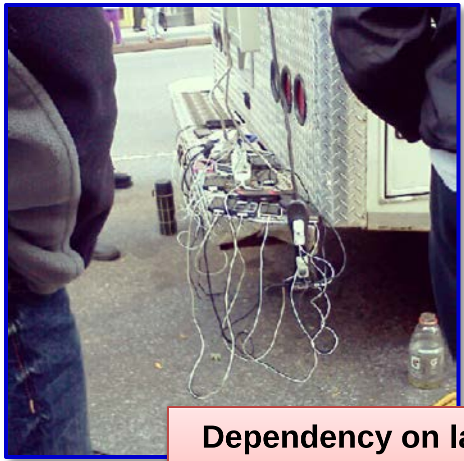


Cutting The Lifeline

The percentage of cellphone-only households is growing

Source: CDC/NCHS surveys of 136,228 households conducted Jan. 2008–Dec 2011; 95% confidence interval

The Wall Street Journal



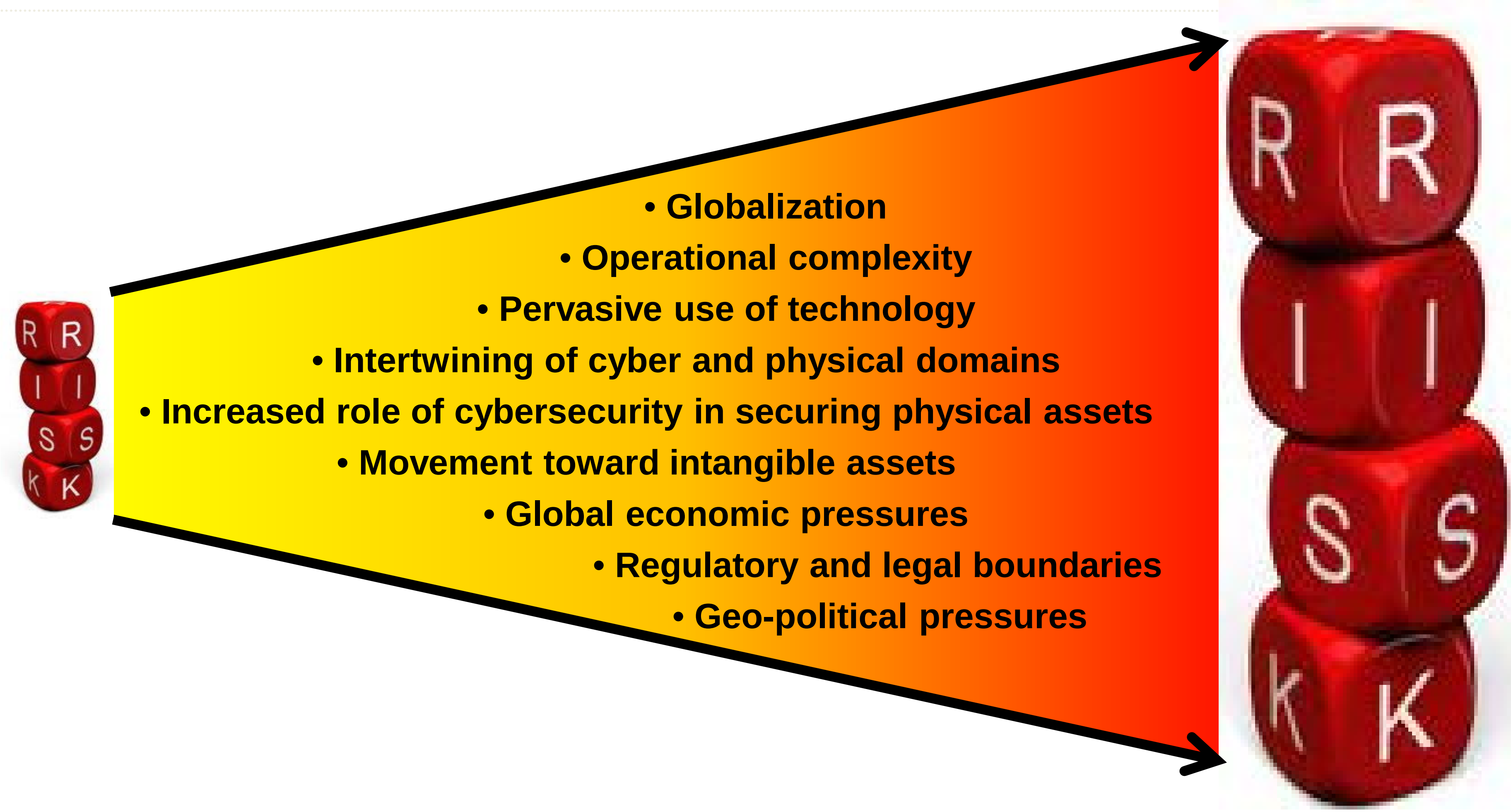
Dependency on large number of mobile devices needing frequent re-charging.

"… As of 2003, 153 million Americans lived in coastal counties - an increase of 33 million since 1980 - and 3.7 million lived within a few feet of high tide…"

-- Bryan Walsh, Time Magazine, November 12, 2012

… and there are many more.

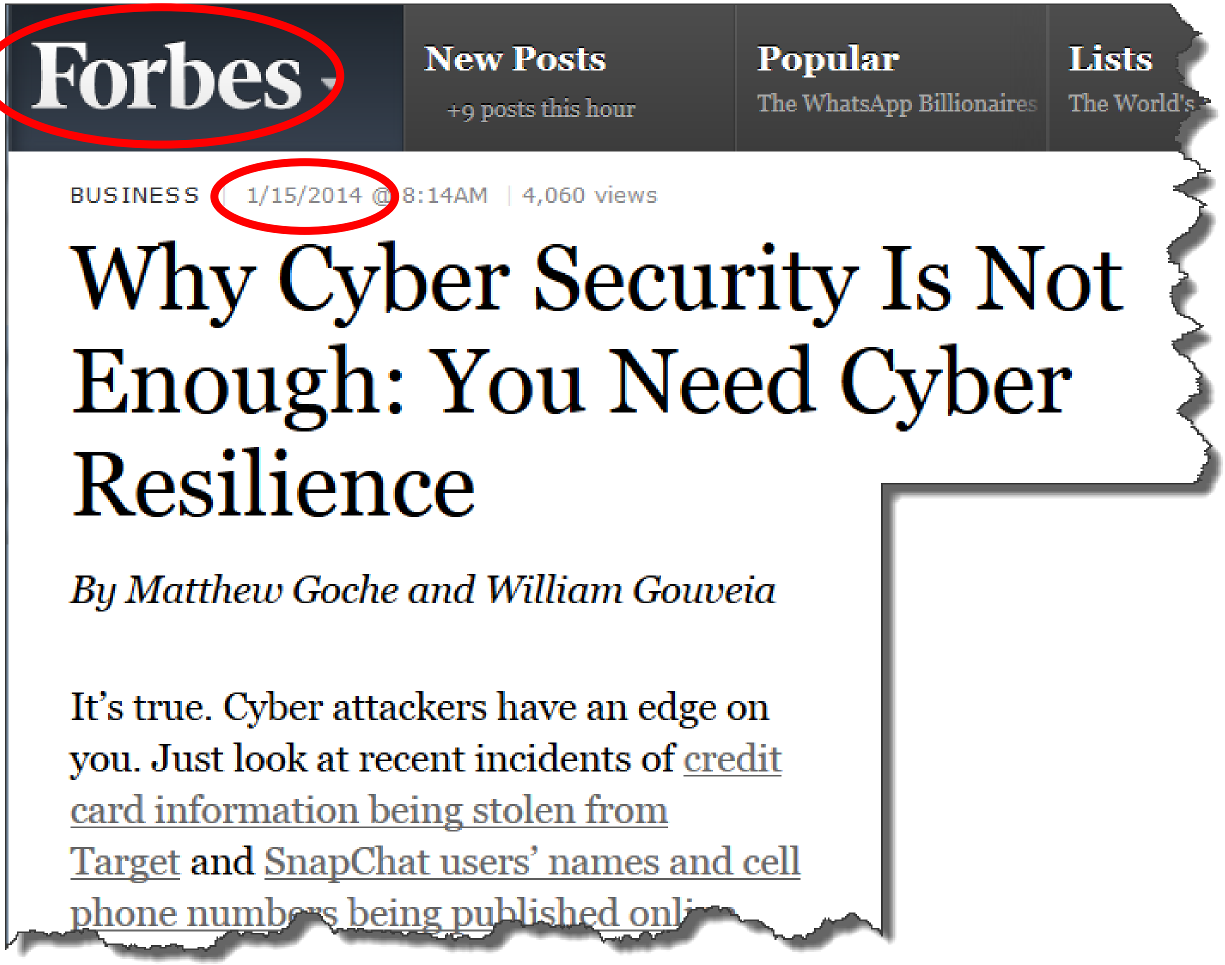
Expansion of Risk Environment



- Globalization
- Operational complexity
- Pervasive use of technology
- Intertwining of cyber and physical domains
- Increased role of cybersecurity in securing physical assets
- Movement toward intangible assets
- Global economic pressures
- Regulatory and legal boundaries
- Geo-political pressures

Successful management of operational risk may require a (significant) shift in thinking and approach.

Interestingly enough…



BUSINESS | 1/15/2014 @ 8:14AM | 4,060 views

Why Cyber Security Is Not Enough: You Need Cyber Resilience

By Matthew Goche and William Gouveia

It's true. Cyber attackers have an edge on you. Just look at recent incidents of credit card information being stolen from Target and SnapChat users' names and cell phone numbers being published onli

A few weeks before they were hacked?

Step-By-Step / Checklist / Roadmap …..

❑

❑ Characterize your risk environment

❑

❑

Organizational Mission

Why are we having this discussion?

American
Red Cross

“The American Red Cross prevents and alleviates human suffering in the face of emergencies by mobilizing the power of volunteers and the generosity of donors.”

- Disaster Relief
- Safe and Adequate Blood Supply
- Health and Safety Education
- ○ ○ ○

UNITED STATES
POSTAL SERVICE

> “To provide postal services to bind the Nation together … To provide prompt, reliable, and efficient services to patrons in all areas and … render postal services to all communities.”

Delivering Mail

Selling Stamps

Ensuring Mail Safety

Operating a 37,000-node intranet

○ ○ ○

Contributing positively to the earth’s natural ecosystem.

Shade

Habitat for Birds

Climbing Opportunity

Beauty

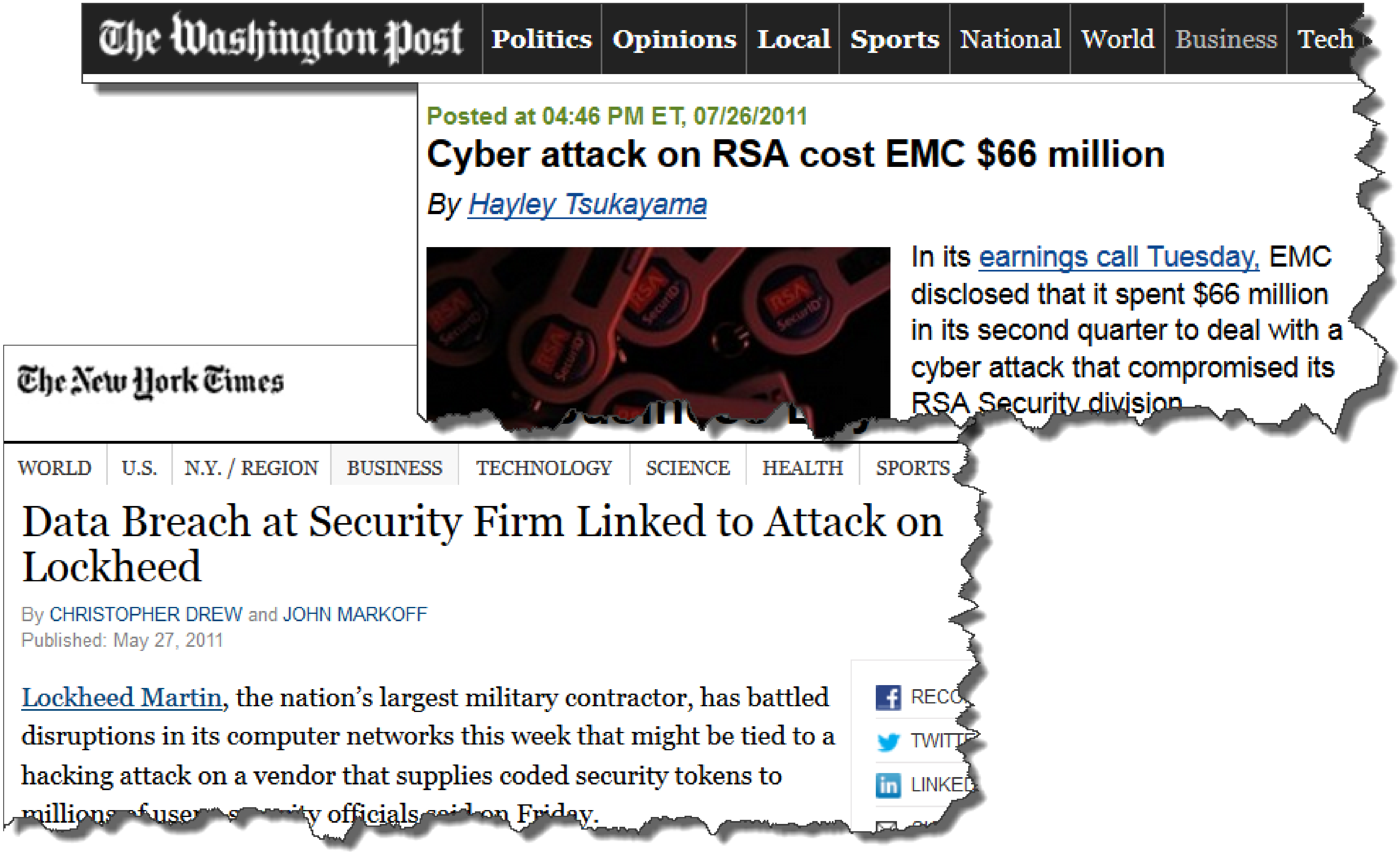
○ ○ ○

Step-By-Step / Checklist / Roadmap …..

- ❑
- ❑ Identify your critical products and services (Why do you exist?)
- ❑ Characterize your risk environment
- ❑
- ❑

Operational Stress

March 2011



The Washington Post

Politics | Opinions | Local | Sports | National | World | Business | Tech

Posted at 04:46 PM ET, 07/26/2011

Cyber attack on RSA cost EMC $66 million

By Hayley Tsukayama

In its earnings call Tuesday, EMC disclosed that it spent $66 million in its second quarter to deal with a cyber attack that compromised its RSA Security division.

The New York Times

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS

Data Breach at Security Firm Linked to Attack on Lockheed

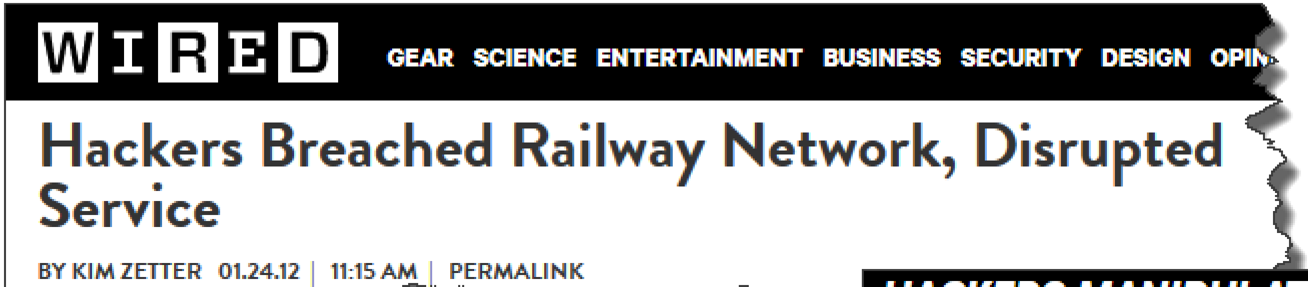
By CHRISTOPHER DREW and JOHN MARKOFF
Published: May 27, 2011

Lockheed Martin, the nation's largest military contractor, has battled disruptions in its computer networks this week that might be tied to a hacking attack on a vendor that supplies coded security tokens to millions of users, security officials said on Friday.

RECO
TWITT
LINKED

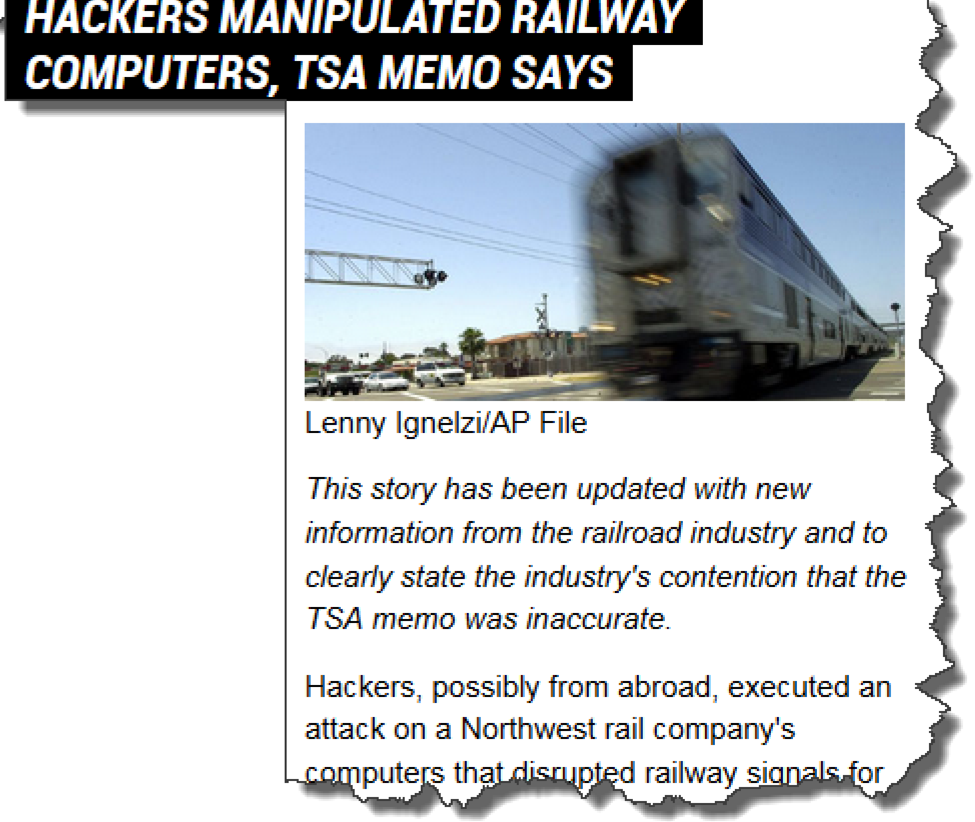
Affecting Customer and Supplier

January 2012



Hackers Breached Railway Network, Disrupted Service

BY KIM ZETTER 01.24.12 | 11:15 AM | PERMALINK



HACKERS MANIPULATED RAILWAY COMPUTERS, TSA MEMO SAYS

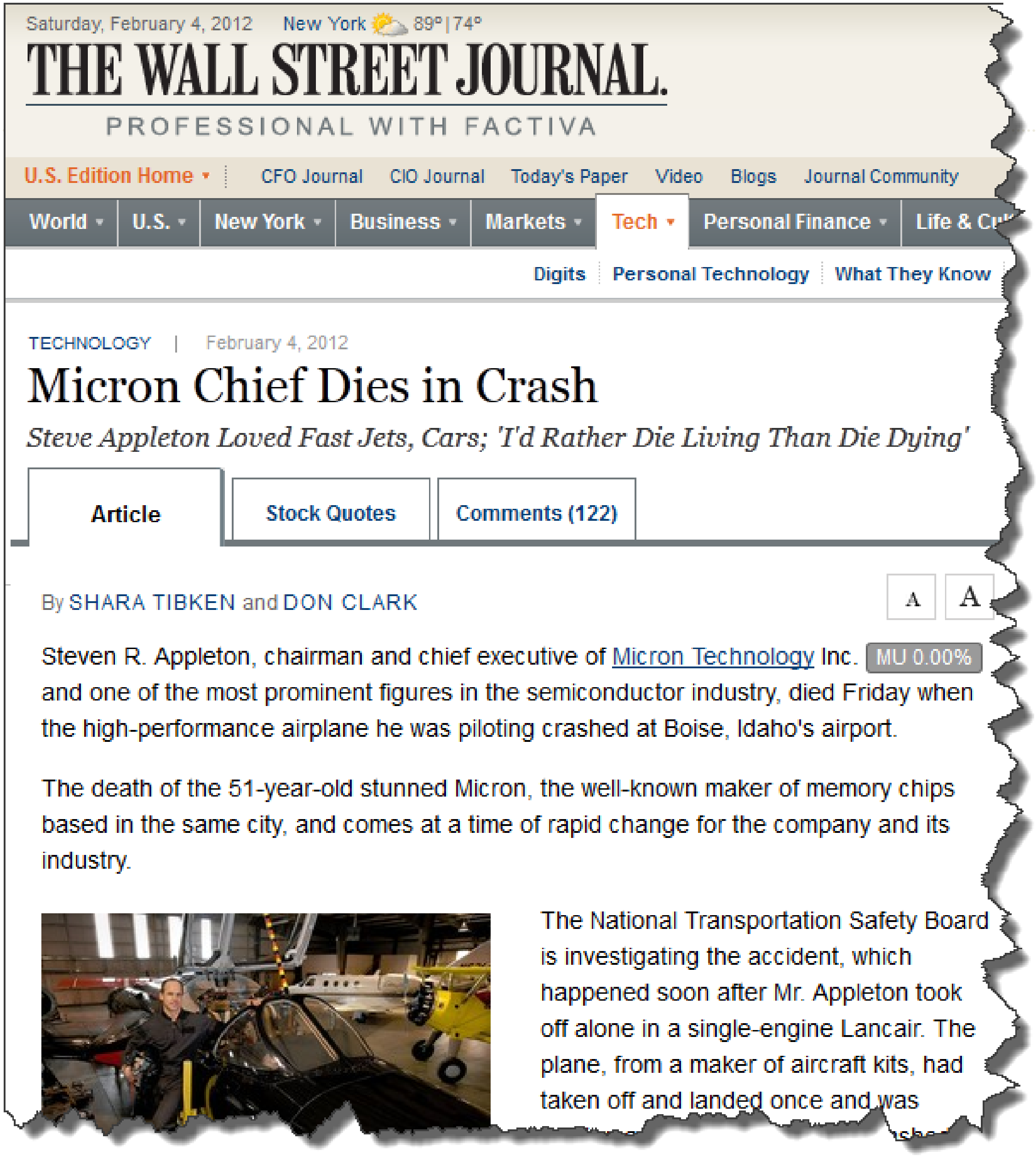
Lenny Ignelzi/AP File

This story has been updated with new information from the railroad industry and to clearly state the industry's contention that the TSA memo was inaccurate.

Hackers, possibly from abroad, executed an attack on a Northwest rail company's computers that disrupted railway signals for

Affecting Health and Safety of Public & Business Ops.

Feb. 2012



Saturday, February 4, 2012 New York 89° | 74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

TECHNOLOGY | February 4, 2012

Micron Chief Dies in Crash

Steve Appleton Loved Fast Jets, Cars; 'I'd Rather Die Living Than Die Dying'

By SHARA TIBKEN and DON CLARK

Steven R. Appleton, chairman and chief executive of Micron Technology Inc. MU 0.00% and one of the most prominent figures in the semiconductor industry, died Friday when the high-performance airplane he was piloting crashed at Boise, Idaho's airport.

The death of the 51-year-old stunned Micron, the well-known maker of memory chips based in the same city, and comes at a time of rapid change for the company and its industry.

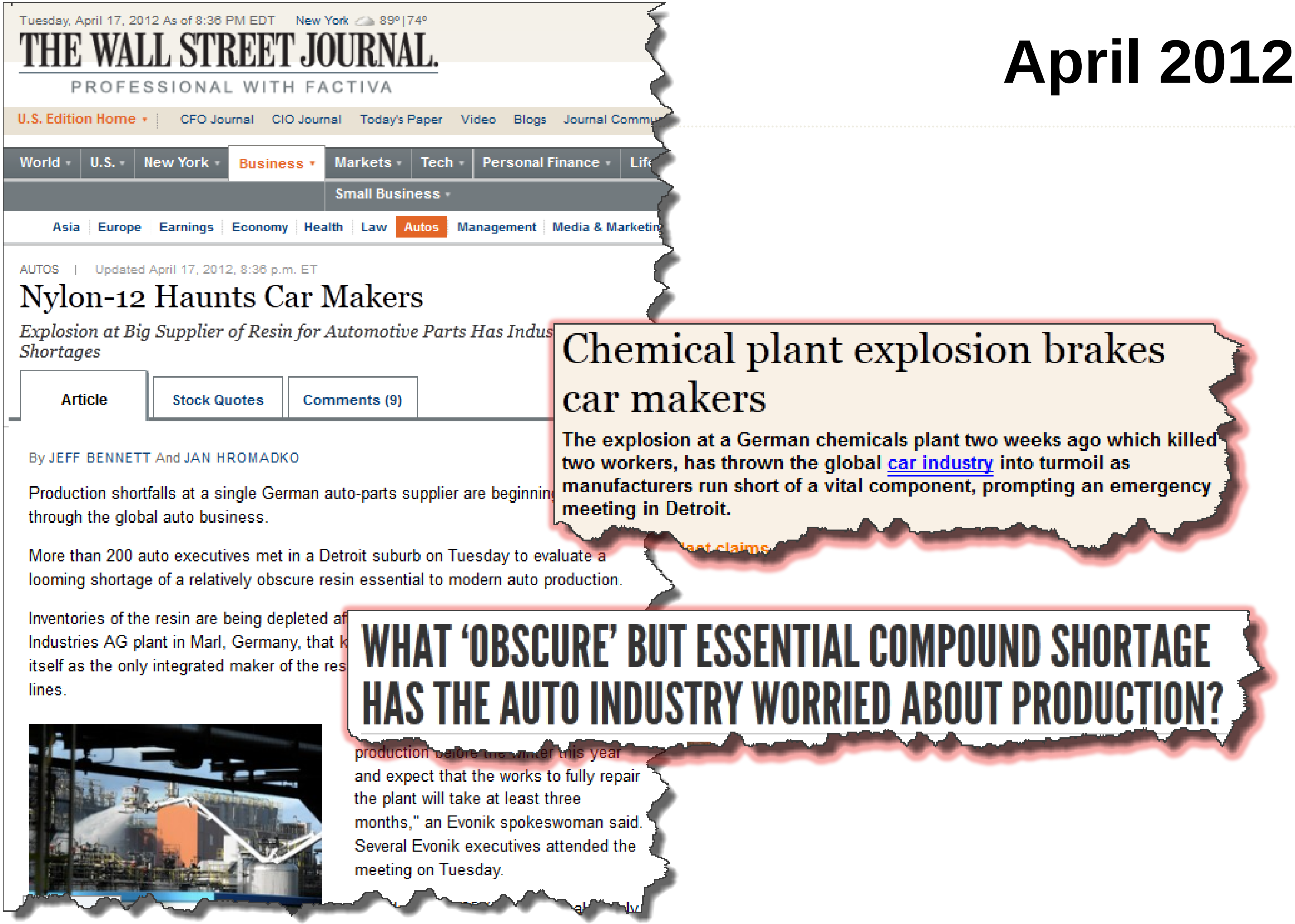
The National Transportation Safety Board is investigating the accident, which happened soon after Mr. Appleton took off alone in a single-engine Lancair. The plane, from a maker of aircraft kits, had taken off and landed once and was

Micron

MICRON TECHNOLOGY, INC.

Unavailability Vital Staff

April 2012



Tuesday, April 17, 2012 As of 8:36 PM EDT New York 89° | 74°

THE WALL STREET JOURNAL.

PROFESSIONAL WITH FACTIVA

AUTOS | Updated April 17, 2012, 8:36 p.m. ET

Nylon-12 Haunts Car Makers

Explosion at Big Supplier of Resin for Automotive Parts Has Indus Shortages

By JEFF BENNETT And JAN HROMADKO

Production shortfalls at a single German auto-parts supplier are beginnin through the global auto business.

More than 200 auto executives met in a Detroit suburb on Tuesday to evaluate a looming shortage of a relatively obscure resin essential to modern auto production.

Inventories of the resin are being depleted af Industries AG plant in Marl, Germany, that k itself as the only integrated maker of the res lines.

production before the winter this year and expect that the works to fully repair the plant will take at least three months," an Evonik spokeswoman said. Several Evonik executives attended the meeting on Tuesday.

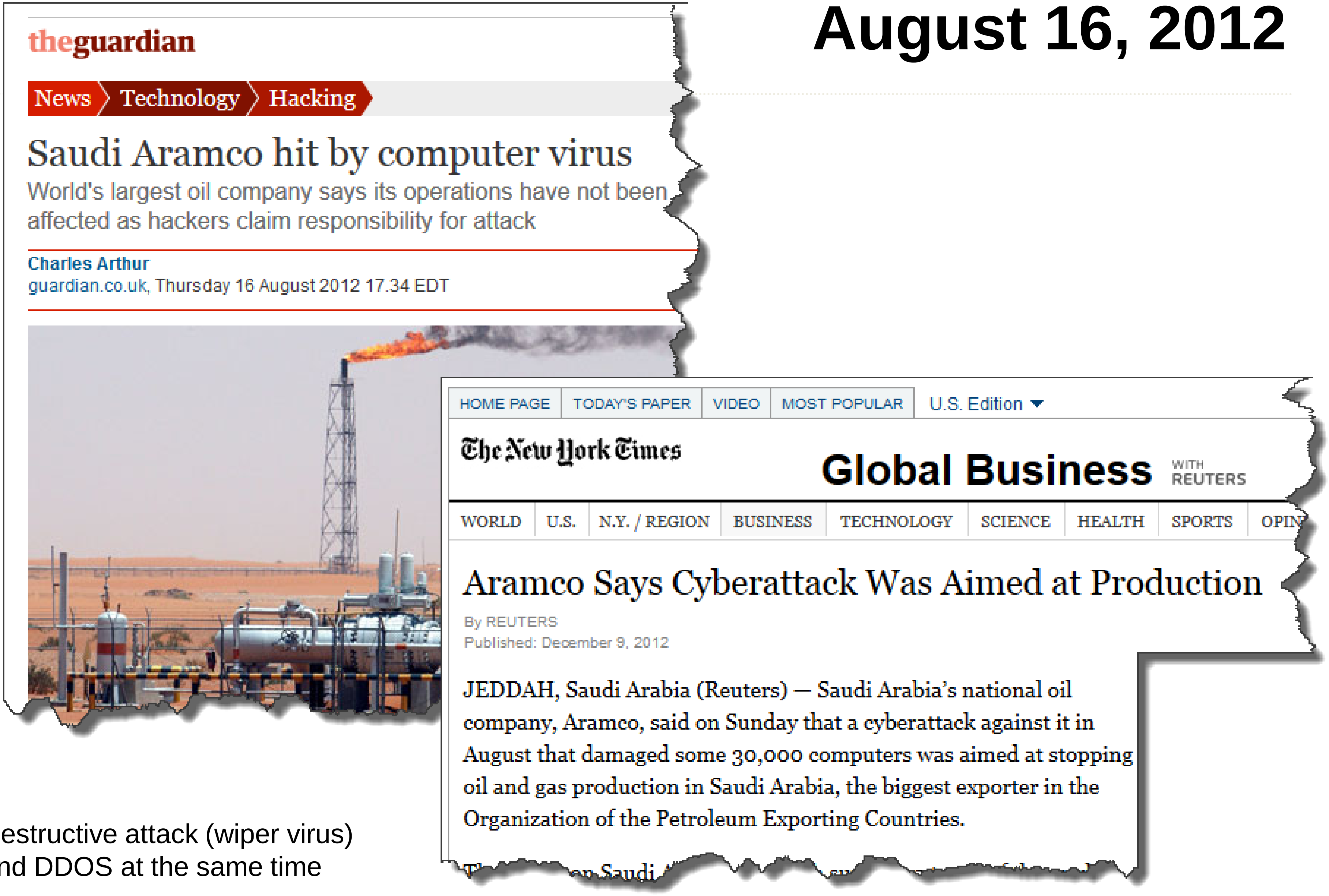
Chemical plant explosion brakes car makers

The explosion at a German chemicals plant two weeks ago which killed two workers, has thrown the global car industry into turmoil as manufacturers run short of a vital component, prompting an emergency meeting in Detroit.

WHAT 'OBSCURE' BUT ESSENTIAL COMPOUND SHORTAGE HAS THE AUTO INDUSTRY WORRIED ABOUT PRODUCTION?

Supply Chain Failures

August 16, 2012



theguardian

News › Technology › Hacking

Saudi Aramco hit by computer virus

World's largest oil company says its operations have not been affected as hackers claim responsibility for attack

Charles Arthur
guardian.co.uk, Thursday 16 August 2012 17.34 EDT

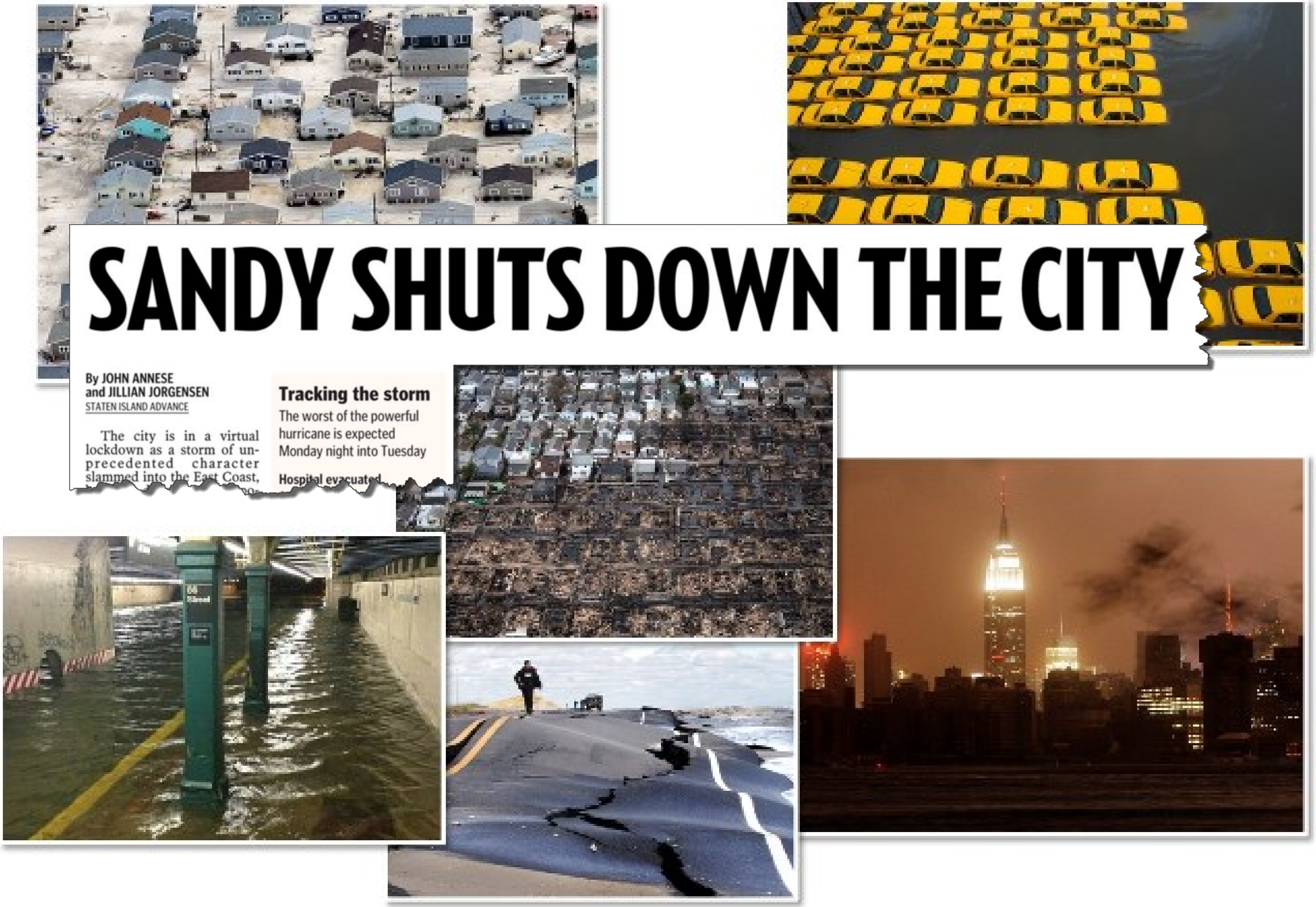
Aramco Says Cyberattack Was Aimed at Production

By REUTERS
Published: December 9, 2012

JEDDAH, Saudi Arabia (Reuters) — Saudi Arabia's national oil company, Aramco, said on Sunday that a cyberattack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia, the biggest exporter in the Organization of the Petroleum Exporting Countries.

Destructive attack (wiper virus)
and DDOS at the same time

Nation-State Cyber Attack on Critical Infrastructure



SANDY SHUTS DOWN THE CITY

By JOHN ANNESE
and JILLIAN JORGENSEN
STATEN ISLAND ADVANCE

The city is in a virtual lockdown as a storm of unprecedented character slammed into the East Coast,

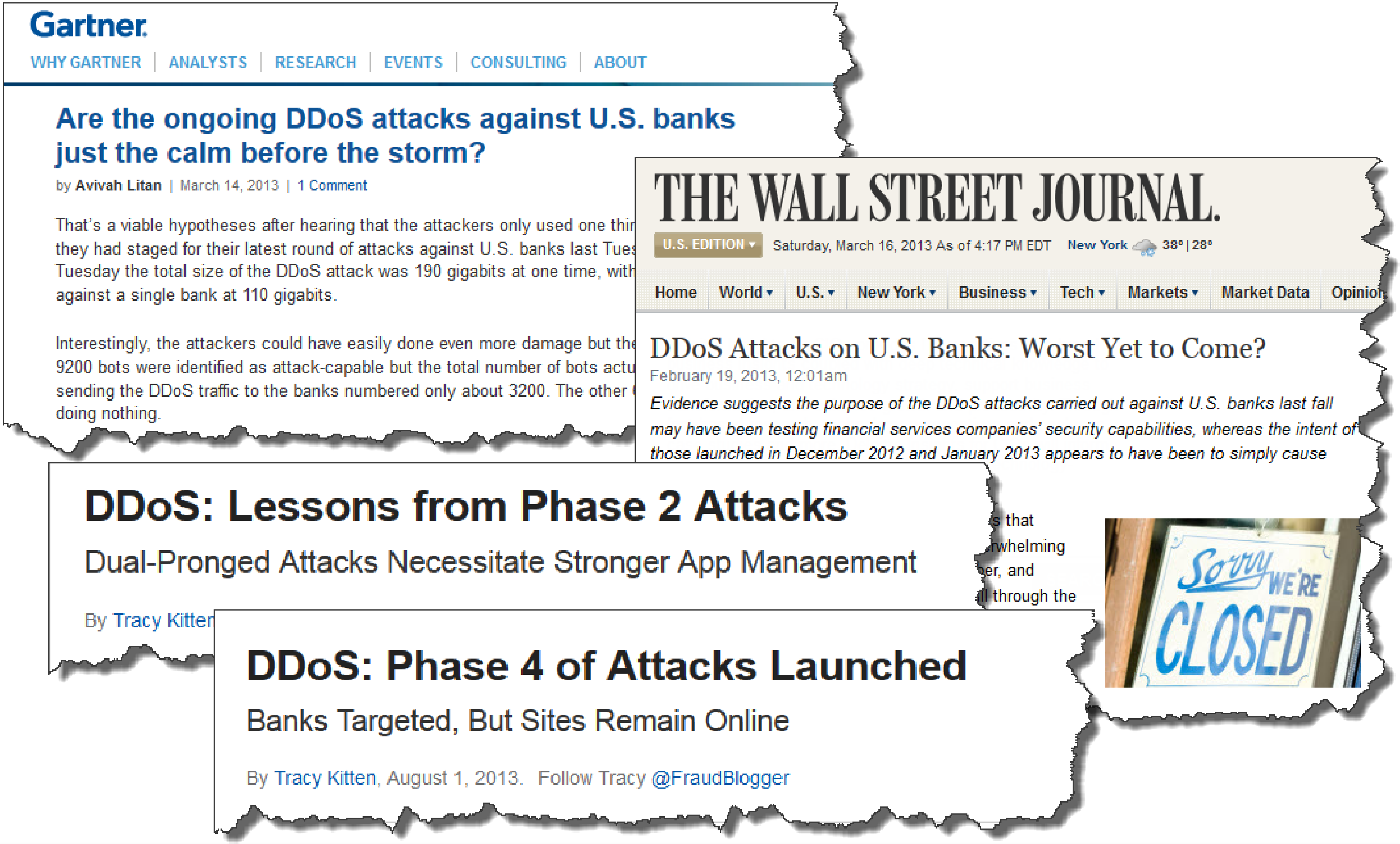
Tracking the storm

The worst of the powerful hurricane is expected Monday night into Tuesday

Hospital evacuated

Natural Disasters Affecting Critical Infrastructure

Late 2012 – Early 2013



Gartner
WHY GARTNER | ANALYSTS | RESEARCH | EVENTS | CONSULTING | ABOUT

Are the ongoing DDoS attacks against U.S. banks just the calm before the storm?

by Avivah Litan | March 14, 2013 | 1 Comment

That's a viable hypotheses after hearing that the attackers only used one thir they had staged for their latest round of attacks against U.S. banks last Tues Tuesday the total size of the DDoS attack was 190 gigabits at one time, with against a single bank at 110 gigabits.

Interestingly, the attackers could have easily done even more damage but the 9200 bots were identified as attack-capable but the total number of bots actu sending the DDoS traffic to the banks numbered only about 3200. The other doing nothing.

THE WALL STREET JOURNAL.
U.S. EDITION ▾
Saturday, March 16, 2013 As of 4:17 PM EDT
New York 38° | 28°
Home | World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Tech ▾ | Markets ▾ | Market Data | Opinio

DDoS Attacks on U.S. Banks: Worst Yet to Come?

February 19, 2013, 12:01am

Evidence suggests the purpose of the DDoS attacks carried out against U.S. banks last fall may have been testing financial services companies' security capabilities, whereas the intent of those launched in December 2012 and January 2013 appears to have been to simply cause

s that
whelming
er, and
ll through the

DDoS: Lessons from Phase 2 Attacks

Dual-Pronged Attacks Necessitate Stronger App Management

By Tracy Kitten

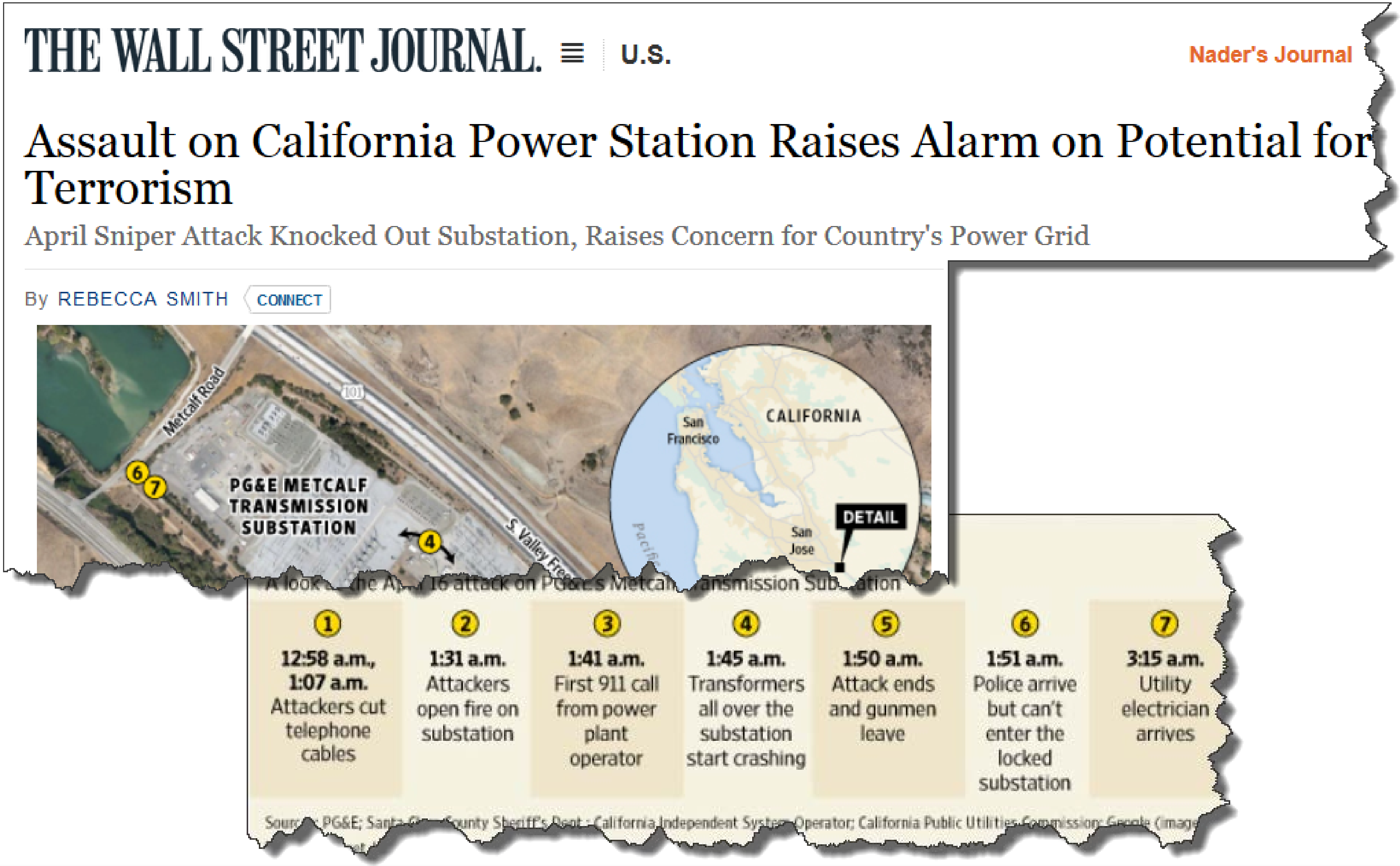
DDoS: Phase 4 of Attacks Launched

Banks Targeted, But Sites Remain Online

By Tracy Kitten, August 1, 2013. Follow Tracy @FraudBlogger

Cyber Attacks on US Financial Industry

April 16, 2013



THE WALL STREET JOURNAL. ≡ U.S.

Nader's Journal

Assault on California Power Station Raises Alarm on Potential for Terrorism

April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid

By REBECCA SMITH CONNECT

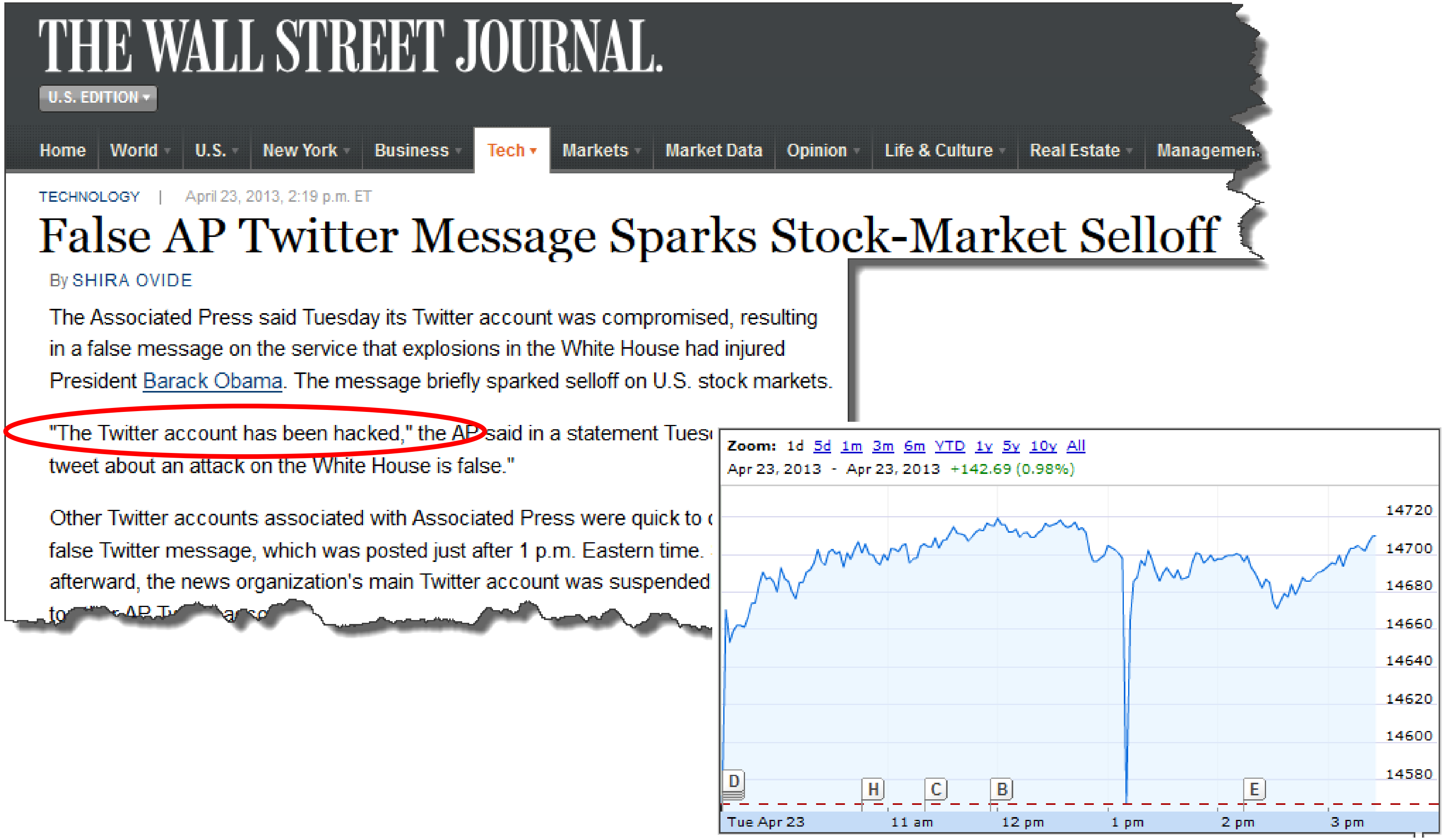
A look at the April 16 attack on PG&E's Metcalf Transmission Substation

1	2	3	4	5	6	7
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack ends and gunmen leave	**1:51 a.m.** Police arrive but can't enter the locked substation	**3:15 a.m.** Utility electrician arrives

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image

Operational Stress on US Electric Grid

April 23, 2013



TECHNOLOGY | April 23, 2013, 2:19 p.m. ET

False AP Twitter Message Sparks Stock-Market Selloff

By SHIRA OVIDE

The Associated Press said Tuesday its Twitter account was compromised, resulting in a false message on the service that explosions in the White House had injured President Barack Obama. The message briefly sparked selloff on U.S. stock markets.

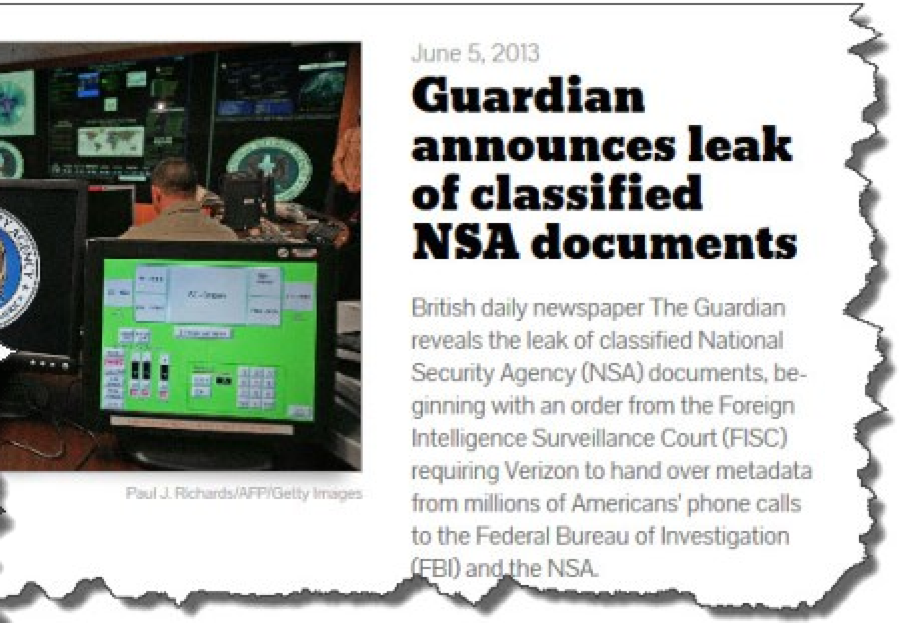
"The Twitter account has been hacked," the AP said in a statement Tues tweet about an attack on the White House is false."

Other Twitter accounts associated with Associated Press were quick to false Twitter message, which was posted just after 1 p.m. Eastern time. afterward, the news organization's main Twitter account was suspended to [illegible]

Zoom: 1d 5d 1m 3m 6m YTD 1y 5y 10y All
Apr 23, 2013 - Apr 23, 2013 +142.69 (0.98%)
14720
14700
14680
14660
14640
14620
14600
14580
D
H
C
B
E
Tue Apr 23
11 am
12 pm
1 pm
2 pm
3 pm

Operational Stress on Financial Markets (& White House)

June 5, 2013

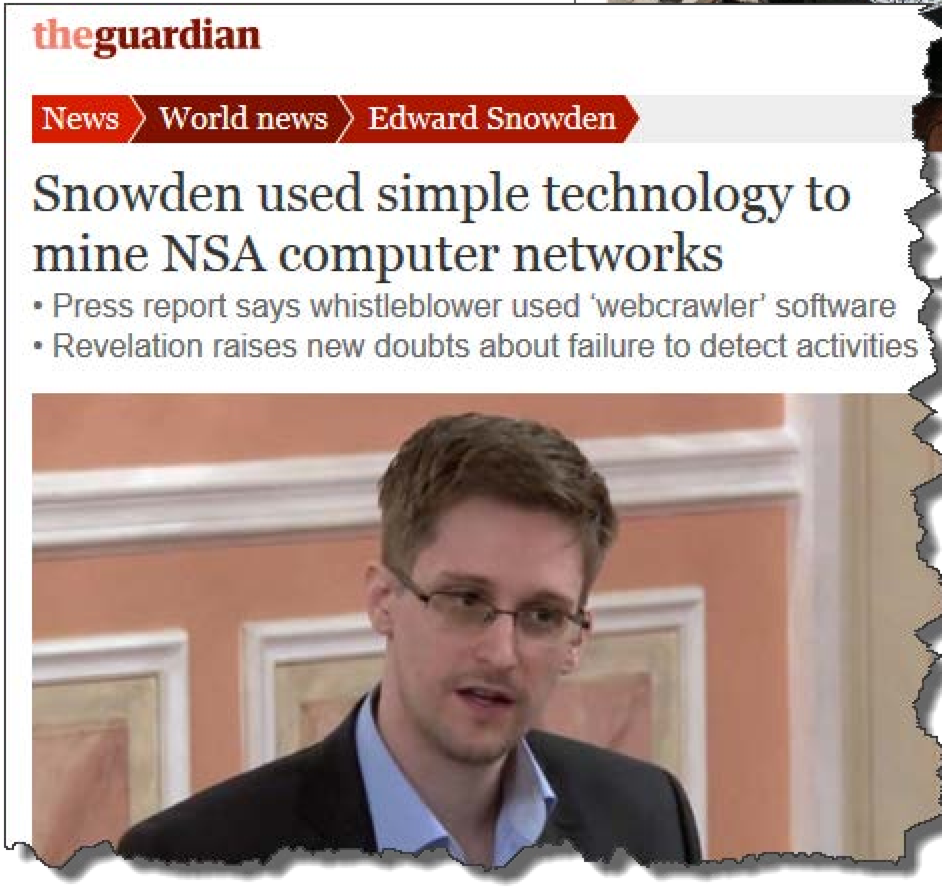


Paul J. Richards/AFP/Getty Images

June 5, 2013

Guardian announces leak of classified NSA documents

British daily newspaper The Guardian reveals the leak of classified National Security Agency (NSA) documents, beginning with an order from the Foreign Intelligence Surveillance Court (FISC) requiring Verizon to hand over metadata from millions of Americans' phone calls to the Federal Bureau of Investigation (FBI) and the NSA.



theguardian

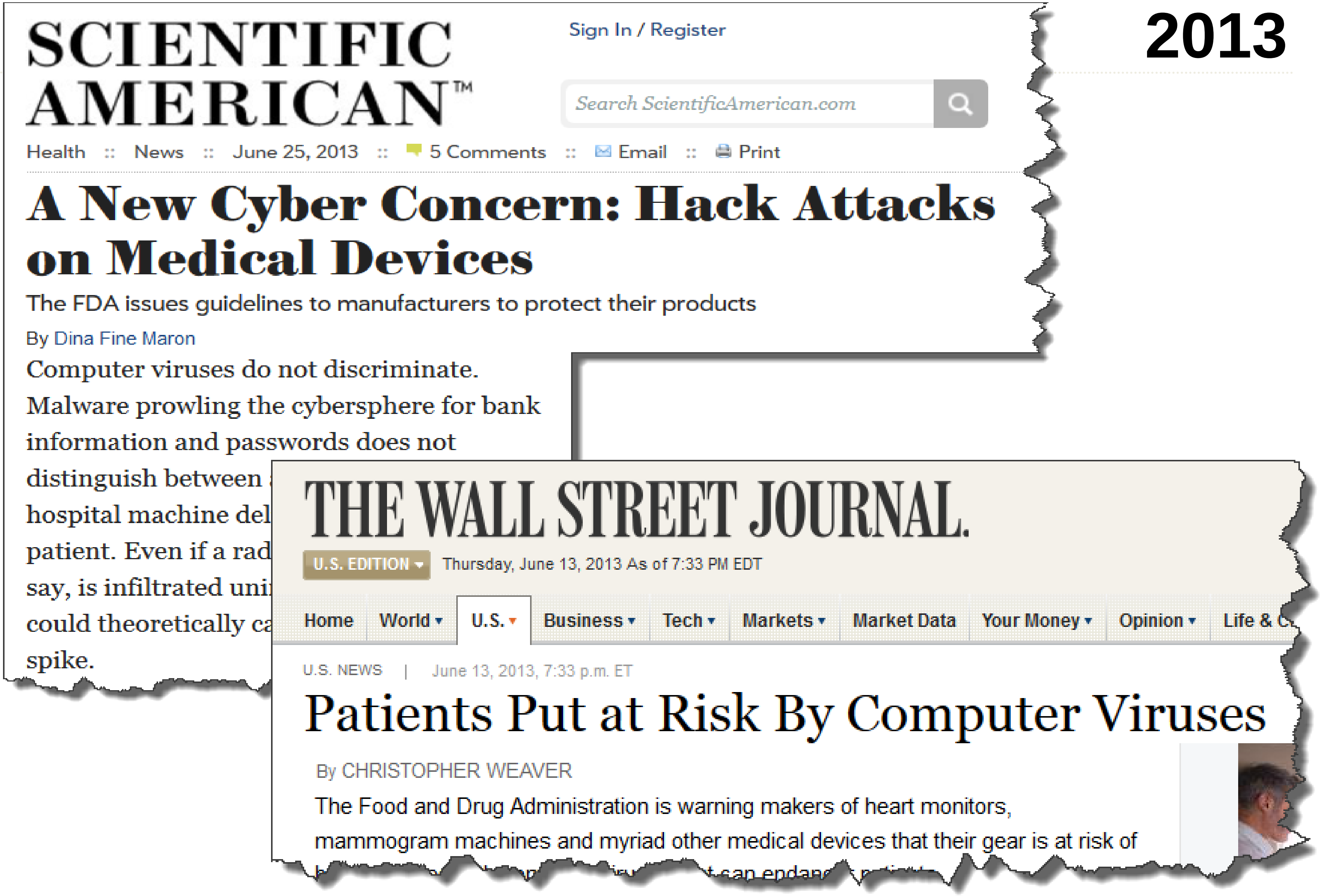
News 〉 World news 〉 Edward Snowden

Snowden used simple technology to mine NSA computer networks

- Press report says whistleblower used 'webcrawler' software
- Revelation raises new doubts about failure to detect activities

Insider Threat

June
2013



SCIENTIFIC AMERICAN™

Sign In / Register

Search ScientificAmerican.com

Health :: News :: June 25, 2013 :: 5 Comments :: Email :: Print

A New Cyber Concern: Hack Attacks on Medical Devices

The FDA issues guidelines to manufacturers to protect their products

By Dina Fine Maron

Computer viruses do not discriminate. Malware prowling the cybersphere for bank information and passwords does not distinguish between a hospital machine del patient. Even if a rad say, is infiltrated uni could theoretically ca spike.

THE WALL STREET JOURNAL.

U.S. EDITION Thursday, June 13, 2013 As of 7:33 PM EDT

U.S. NEWS | June 13, 2013, 7:33 p.m. ET

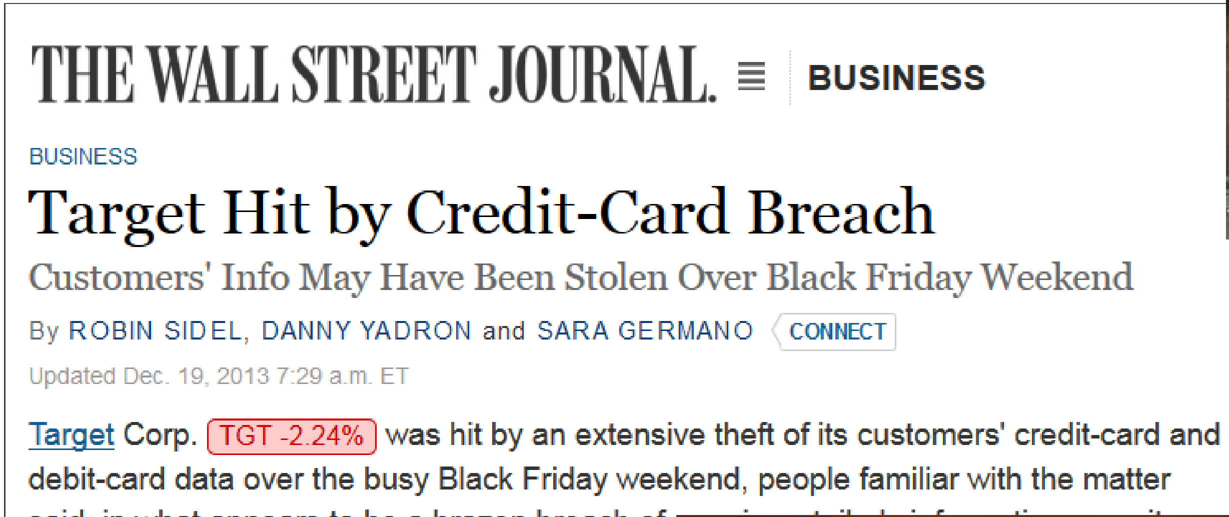
Patients Put at Risk By Computer Viruses

By CHRISTOPHER WEAVER

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of

Intertwining of Physical (Medical) and Cyber World

December 2013



THE WALL STREET JOURNAL. ≡ BUSINESS

BUSINESS

Target Hit by Credit-Card Breach

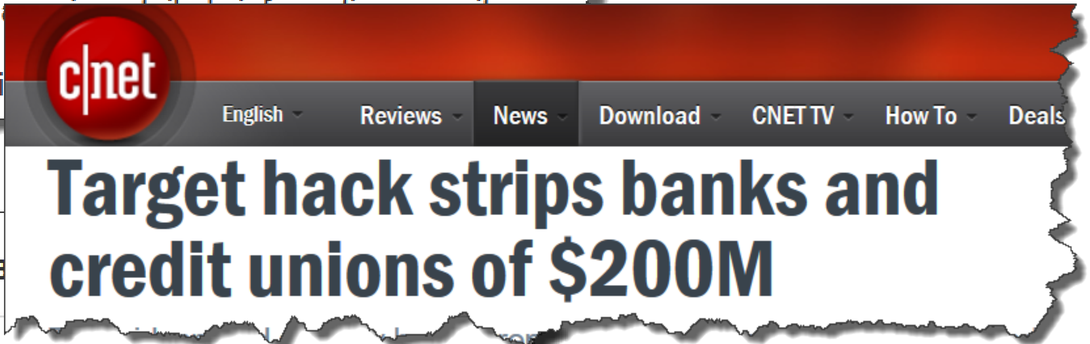
Customers' Info May Have Been Stolen Over Black Friday Weekend

By ROBIN SIDEL, DANNY YADRON and SARA GERMANO CONNECT

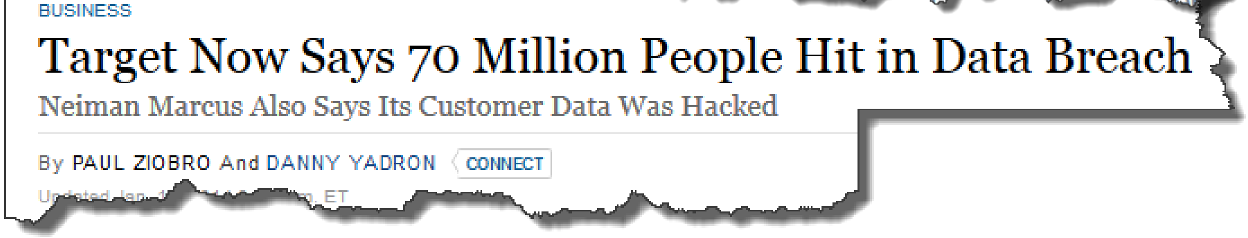
Updated Dec. 19, 2013 7:29 a.m. ET

Target Corp. TGT -2.24% was hit by an extensive theft of its customers' credit-card and debit-card data over the busy Black Friday weekend, people familiar with the matter said, in what appears to be a brazen breach of

The theft was national in scope and happened i



Target hack strips banks and credit unions of $200M



THE WALL STREET JOURNAL. ≡ B

BUSINESS

Target Now Says 70 Million People Hit in Data Breach

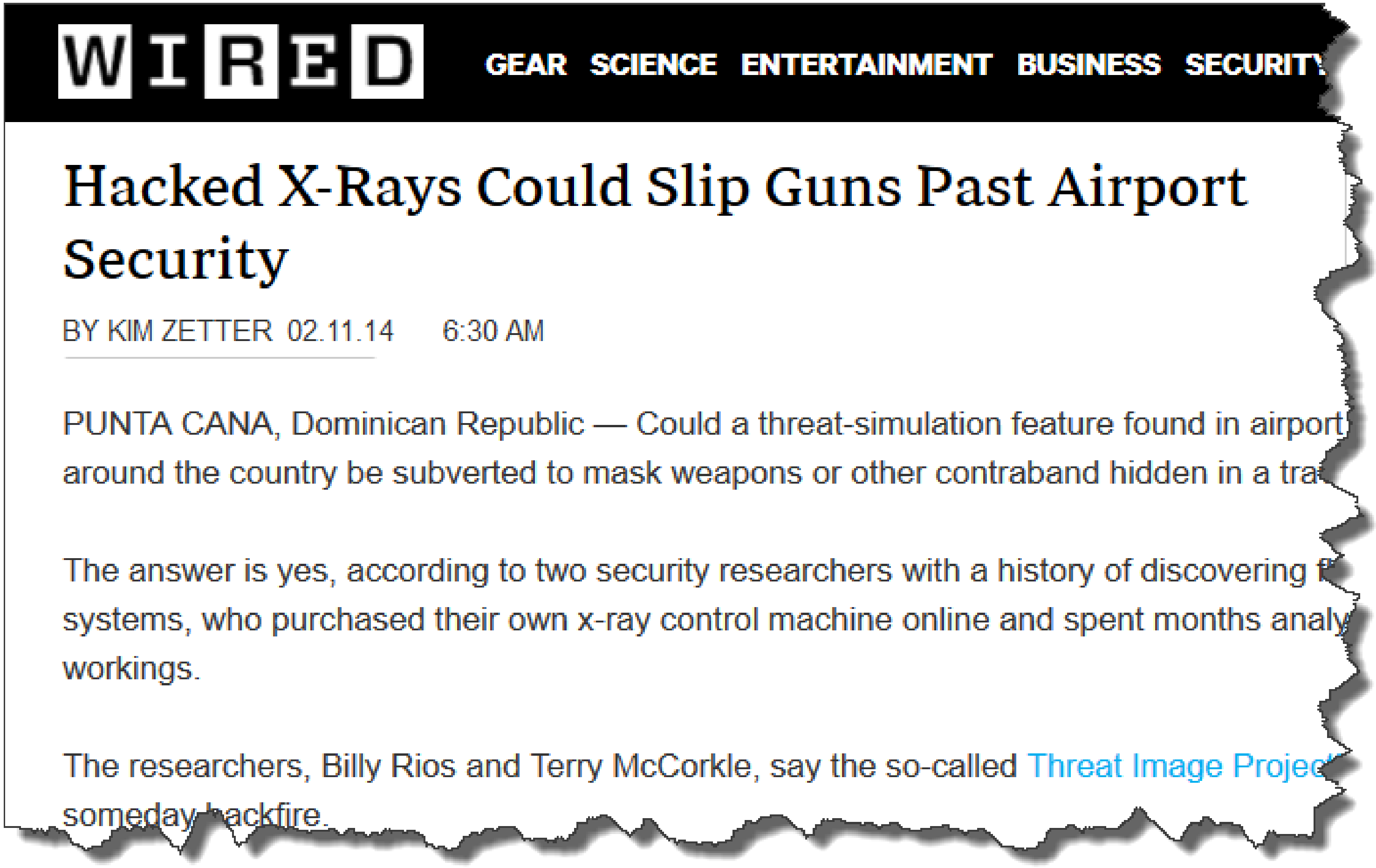
Neiman Marcus Also Says Its Customer Data Was Hacked

By PAUL ZIOBRO And DANNY YADRON CONNECT

Updated Jan. 1 [illegible] m. ET

Operational Stress on Target and its Customers

February 11, 2014



Hacked X-Rays Could Slip Guns Past Airport Security

BY KIM ZETTER 02.11.14 6:30 AM

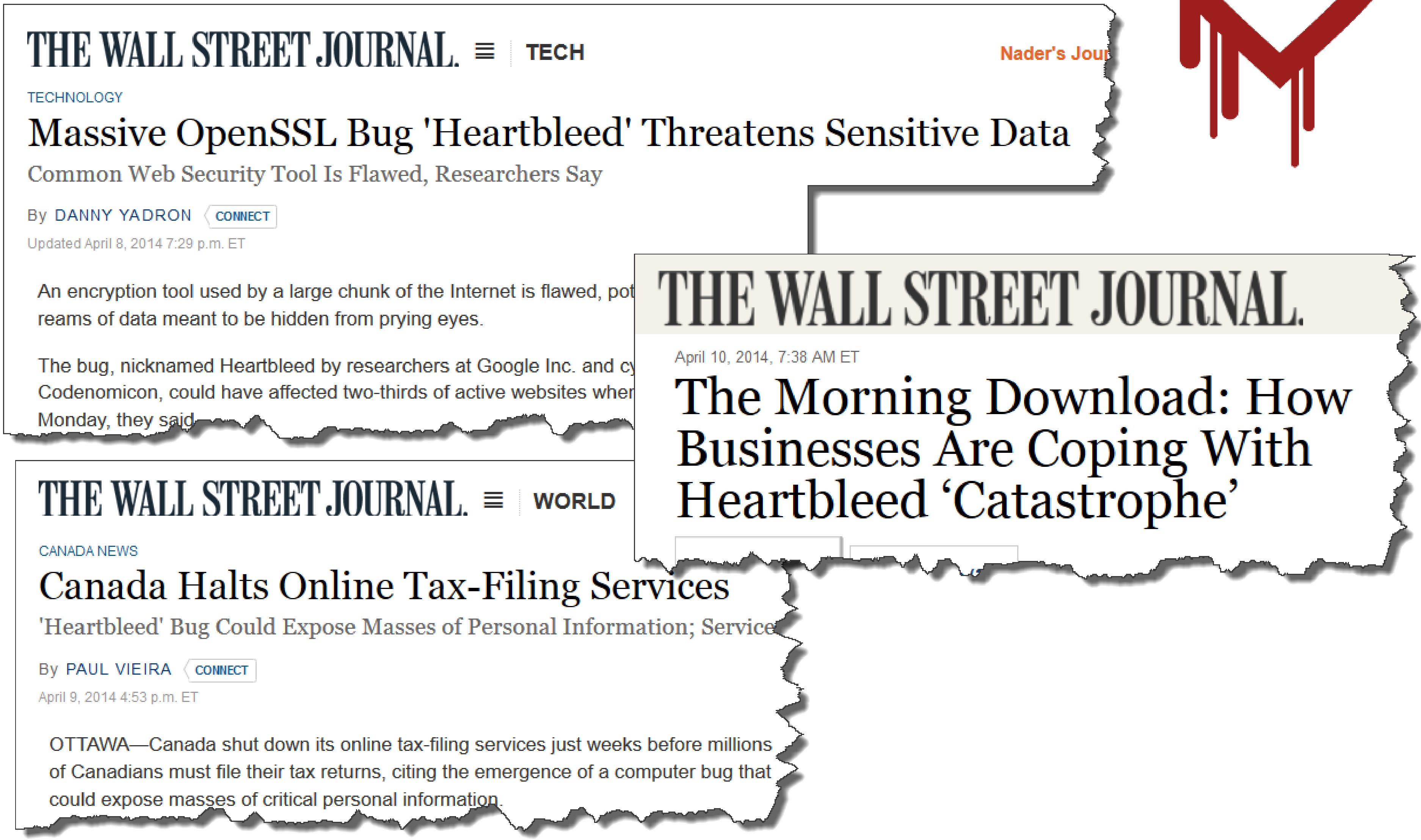
PUNTA CANA, Dominican Republic — Could a threat-simulation feature found in airport around the country be subverted to mask weapons or other contraband hidden in a tra

The answer is yes, according to two security researchers with a history of discovering f systems, who purchased their own x-ray control machine online and spent months analy workings.

The researchers, Billy Rios and Terry McCorkle, say the so-called Threat Image Project someday backfire.

Intertwining of Physical and Cyber World

April 2014



THE WALL STREET JOURNAL. ≡ TECH

Nader's Jour

TECHNOLOGY

Massive OpenSSL Bug 'Heartbleed' Threatens Sensitive Data

Common Web Security Tool Is Flawed, Researchers Say

By DANNY YADRON CONNECT

Updated April 8, 2014 7:29 p.m. ET

An encryption tool used by a large chunk of the Internet is flawed, pot
reams of data meant to be hidden from prying eyes.

The bug, nicknamed Heartbleed by researchers at Google Inc. and cy
Codenomicon, could have affected two-thirds of active websites wher
Monday, they said.

THE WALL STREET JOURNAL.

April 10, 2014, 7:38 AM ET

The Morning Download: How Businesses Are Coping With Heartbleed 'Catastrophe'

THE WALL STREET JOURNAL. ≡ WORLD

CANADA NEWS

Canada Halts Online Tax-Filing Services

'Heartbleed' Bug Could Expose Masses of Personal Information; Service

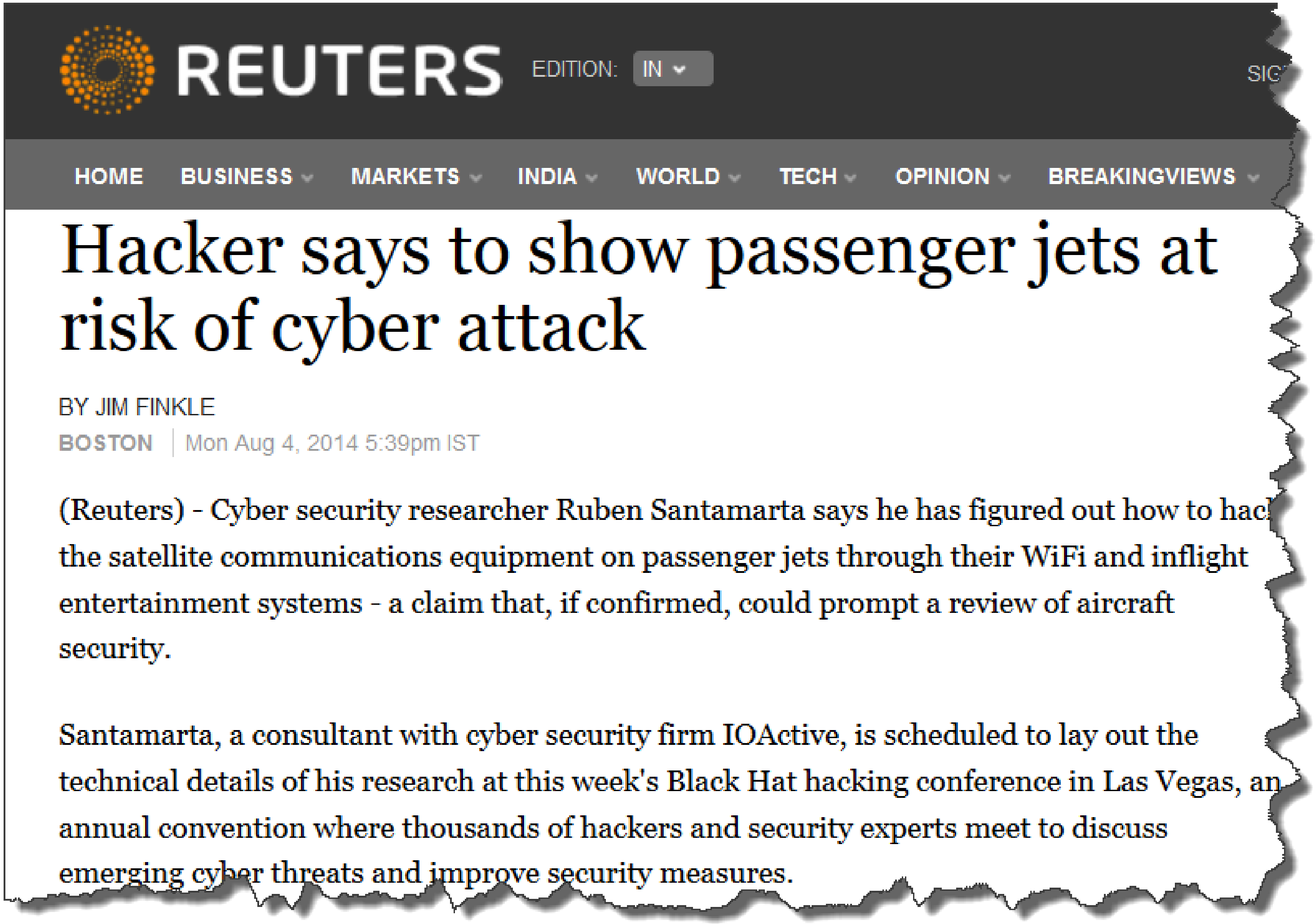
By PAUL VIEIRA CONNECT

April 9, 2014 4:53 p.m. ET

OTTAWA—Canada shut down its online tax-filing services just weeks before millions of Canadians must file their tax returns, citing the emergence of a computer bug that could expose masses of critical personal information.

Operational Stress on Internet and eCommerce

August 4, 2014



Hacker says to show passenger jets at risk of cyber attack

BY JIM FINKLE

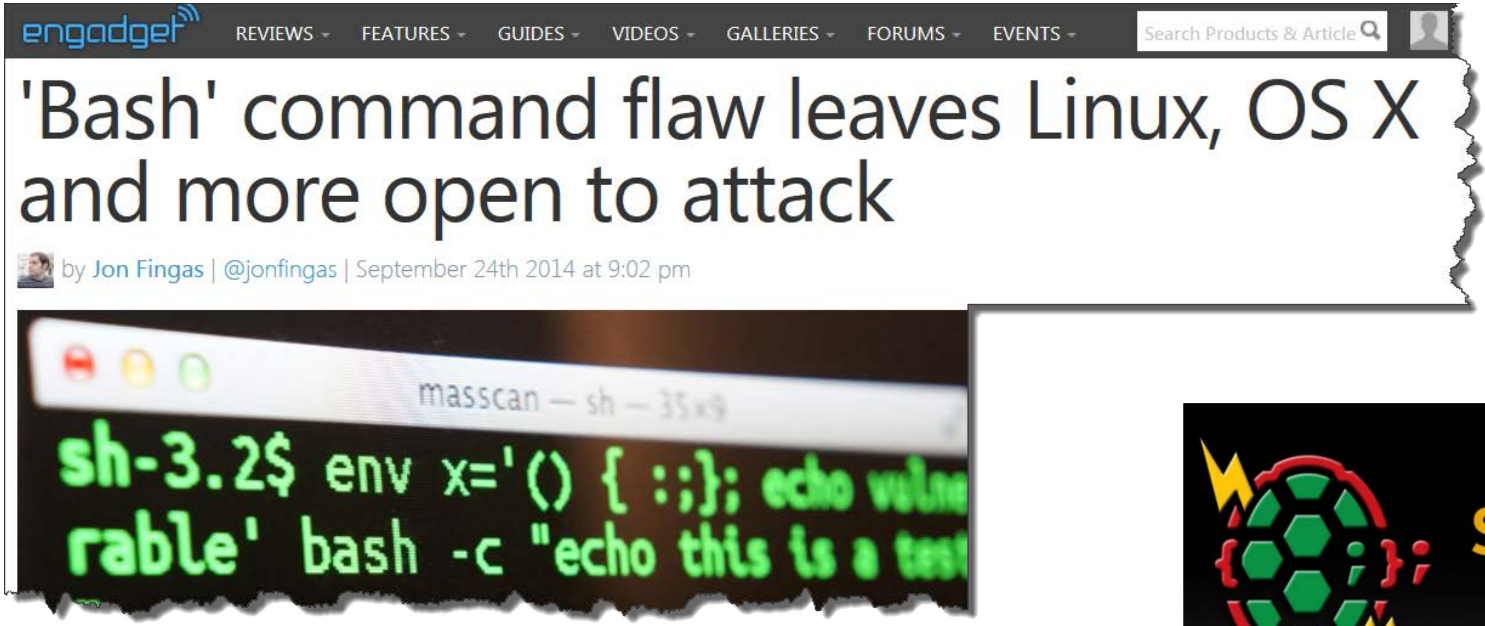
BOSTON | Mon Aug 4, 2014 5:39pm IST

(Reuters) - Cyber security researcher Ruben Santamarta says he has figured out how to hac the satellite communications equipment on passenger jets through their WiFi and inflight entertainment systems - a claim that, if confirmed, could prompt a review of aircraft security.

Santamarta, a consultant with cyber security firm IOActive, is scheduled to lay out the technical details of his research at this week's Black Hat hacking conference in Las Vegas, an annual convention where thousands of hackers and security experts meet to discuss emerging cyber threats and improve security measures.

Stress on Traveling Public, Air Carriers, TSA, …

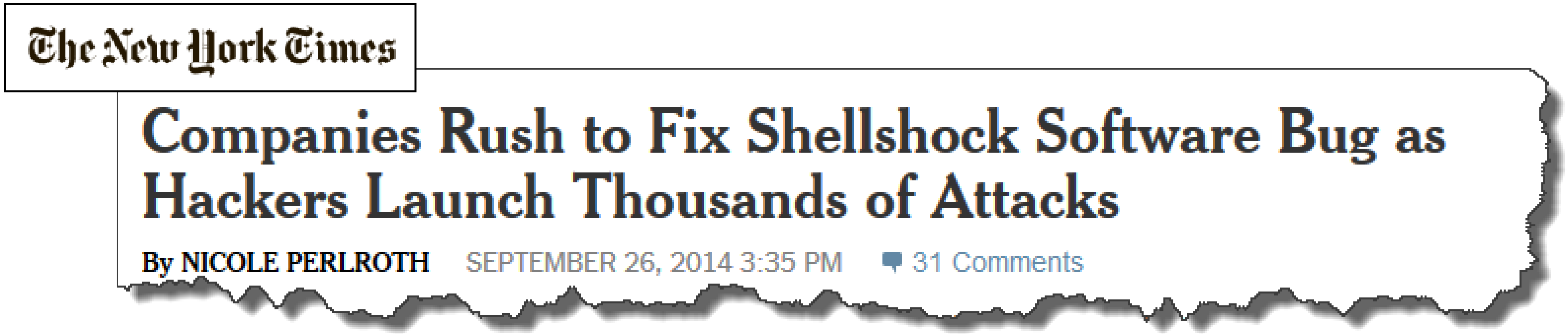
September 24, 2014



'Bash' command flaw leaves Linux, OS X and more open to attack

by Jon Fingas | @jonfingas | September 24th 2014 at 9:02 pm

```
masscan — sh — 35x9
sh-3.2$ env x='() { :;}; echo vulne
rable' bash -c "echo this is a tes
```



Companies Rush to Fix Shellshock Software Bug as Hackers Launch Thousands of Attacks

By NICOLE PERLROTH SEPTEMBER 26, 2014 3:35 PM 31 Comments

Operational Stress on Internet and eCommerce

Step-By-Step / Checklist / Roadmap …..

❑

❑ Identify your critical products and services (Why do you exist?)

❑ What dose operational stress mean to you?

❑ Characterize your risk environment

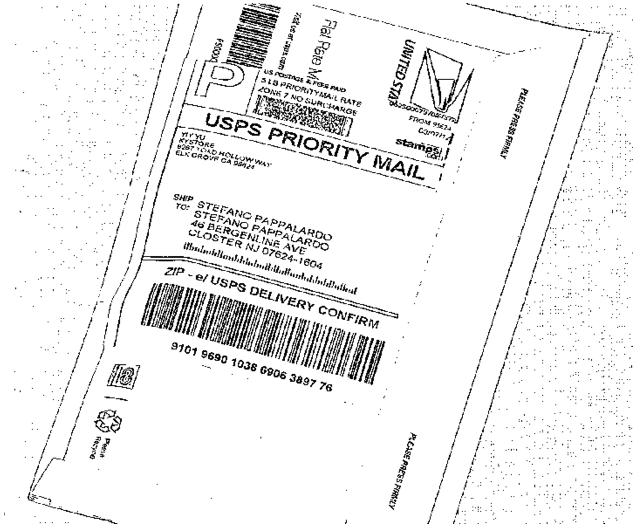
❑

❑

EXAMPLE:
Operational Stress for USPS – White Powder

Operational Risk: Safety & Availability of People Assets

EXAMPLE :
Operational Stress for USPS – Bad Postage



Flat Rate M

US POSTAGE & FEES PAID
5 LB PRIORITY MAIL RATE
ZONE 7 NO SURCHARGE

UNITED STA

FROM 95624

stamps.com

USPS PRIORITY MAIL

YIY YU
KYSTORE
9287 TOAD HOLLOW WAY
ELK GROVE CA 95624

SHIP TO: STEFANO PAPPALARDO
STEFANO PAPPALARDO
46 BERGENLINE AVE
CLOSTER NJ 07624-1604

ZIP - e/ USPS DELIVERY CONFIRM

9101 9690 1036 6906 3897 76

PLEASE PRESS FIRMLY

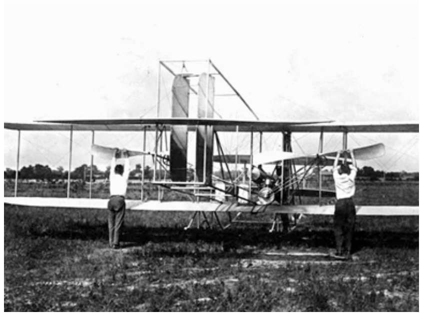
PLEASE PRESS FIRMLY

- Short pay
- Reused
- Photoshopped
- Counterfeit
- Photocopied

Operational Risk: Operational Inefficiencies; Revenue Assurance

Yesterday vs. Today

Ever-Increasing Capability & Complexity



Biplane

0 SLOC

Apollo Lunar Module

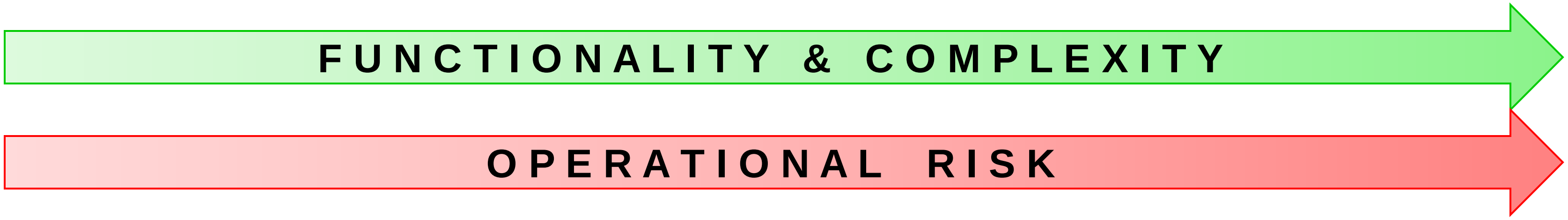
2K SLOC

SR-71

500K SLOC

F-35

9.9M SLOC

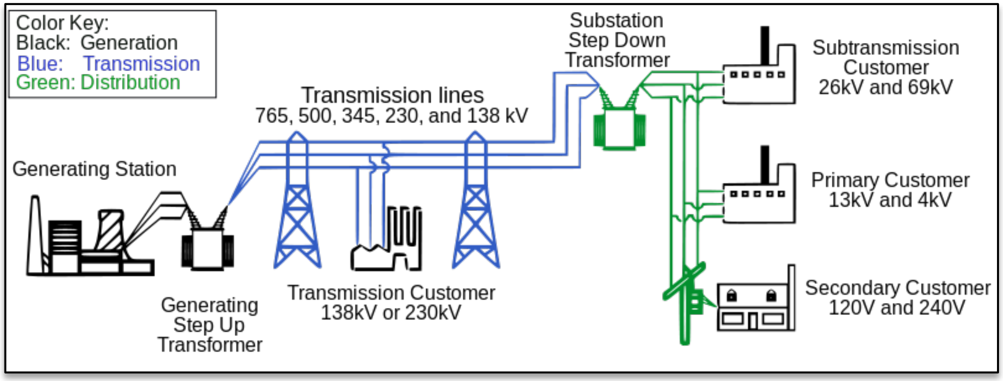


FUNCTIONALITY & COMPLEXITY

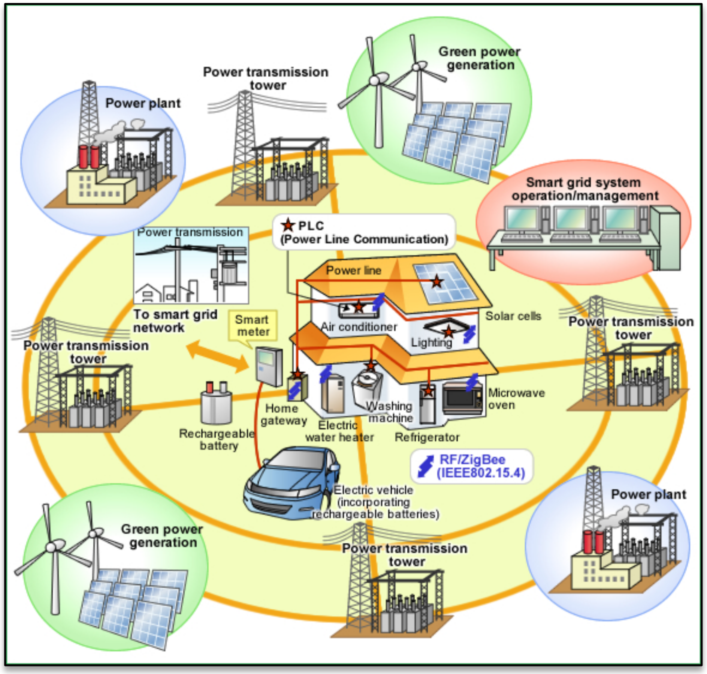
OPERATIONAL RISK

SLOC = Source Lines of Code

Ever-Increasing Capability & Complexity



Legacy Electric Grid

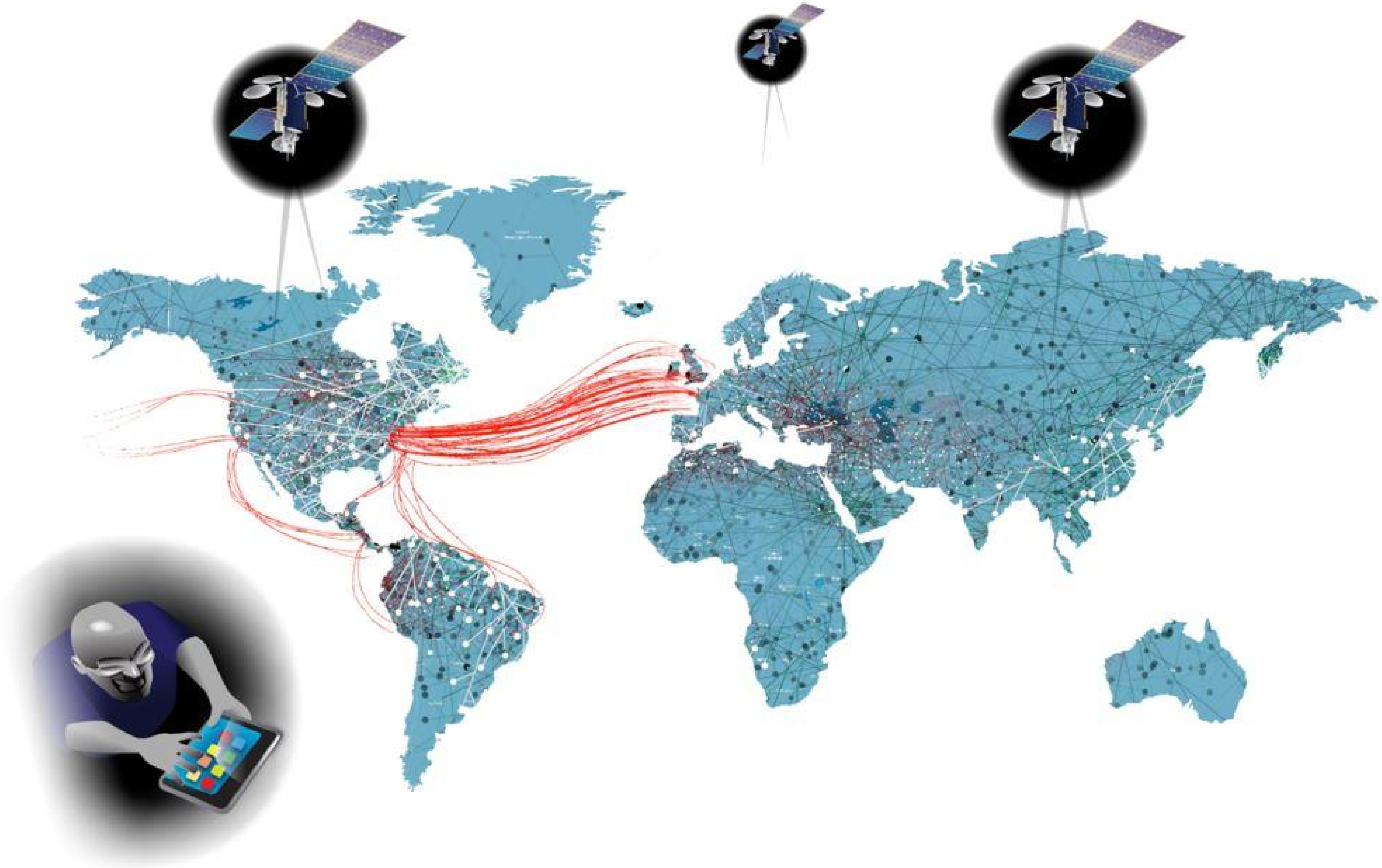


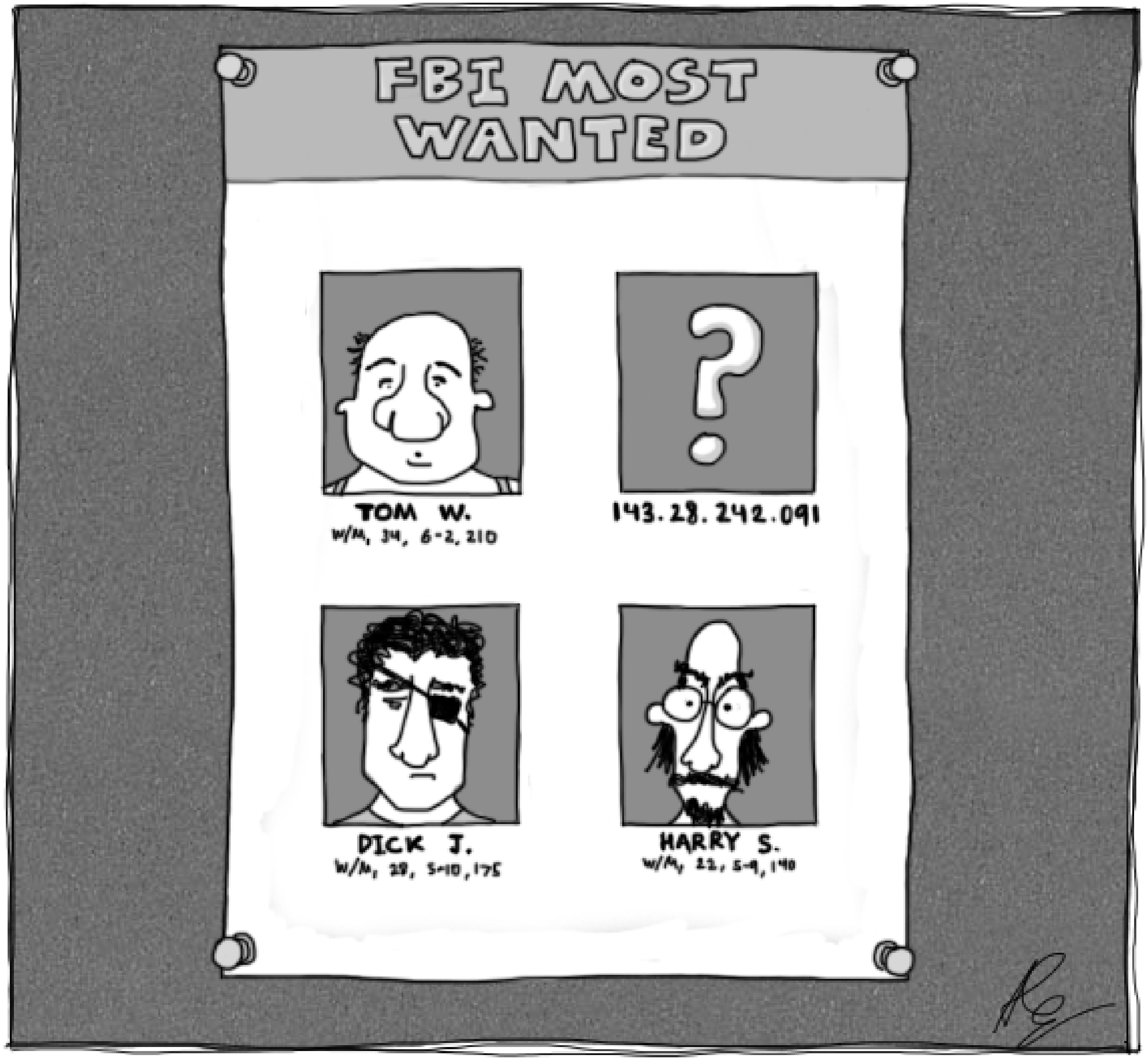
Modern Smart Grid

FUNCTIONALITY & EFFICIENCY

OPERATIONAL RISK

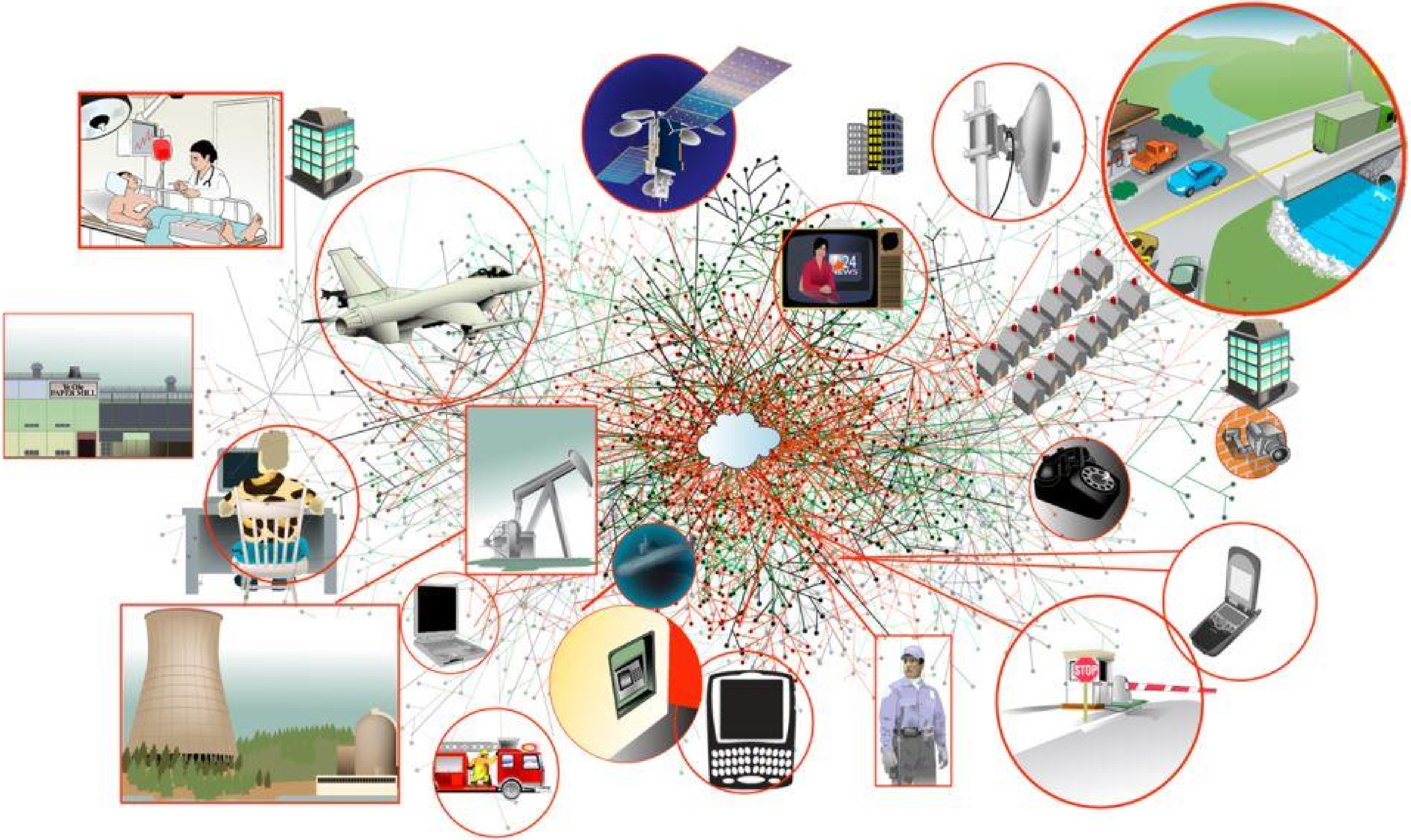
Geographic Boundaries Disappear in Cyberspace



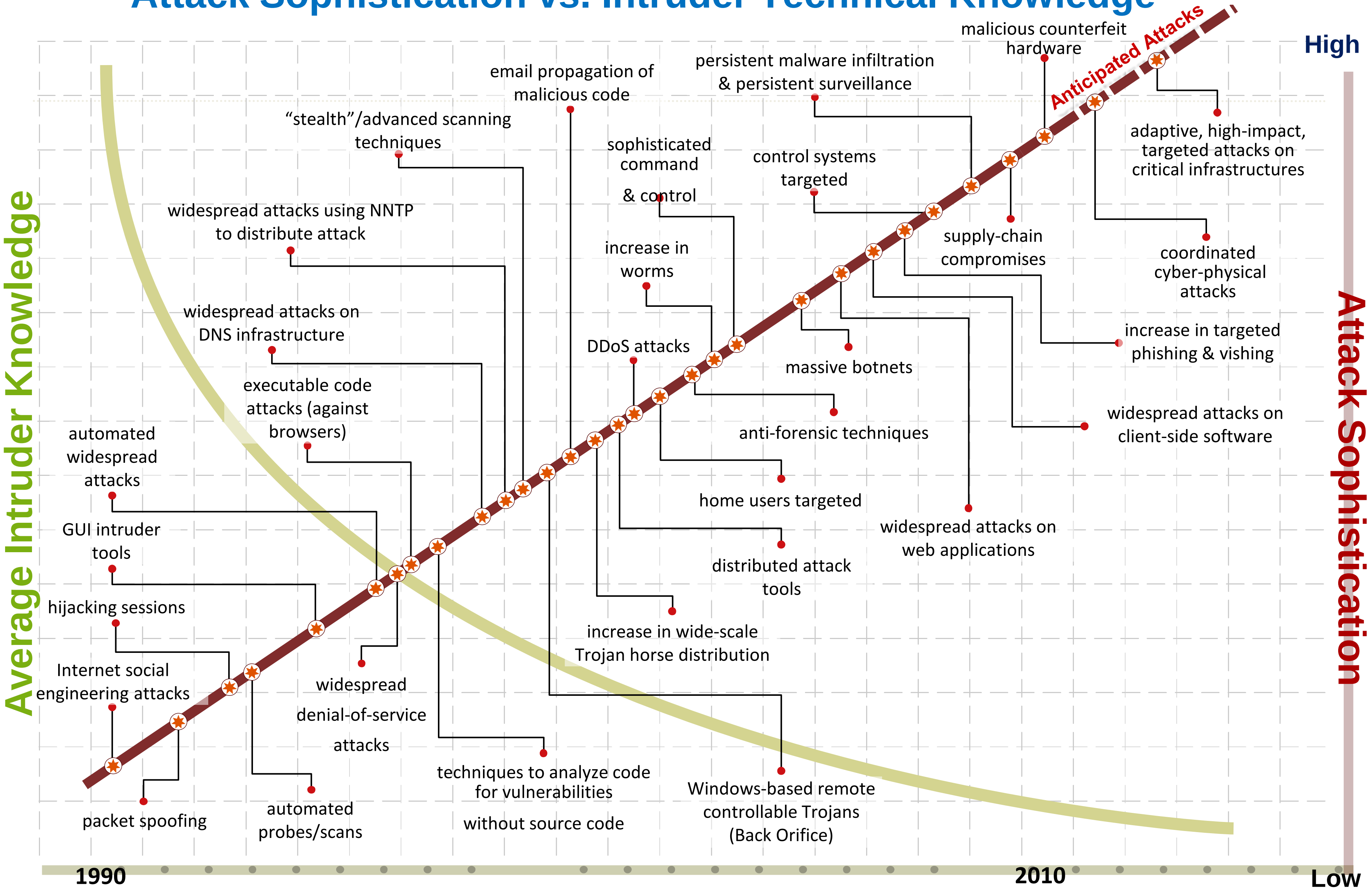


http://www.threatgeek.com/2012/06/threattoons-fbi-most-wanted.html

We Depend on Evolving Cyber Ecosystems



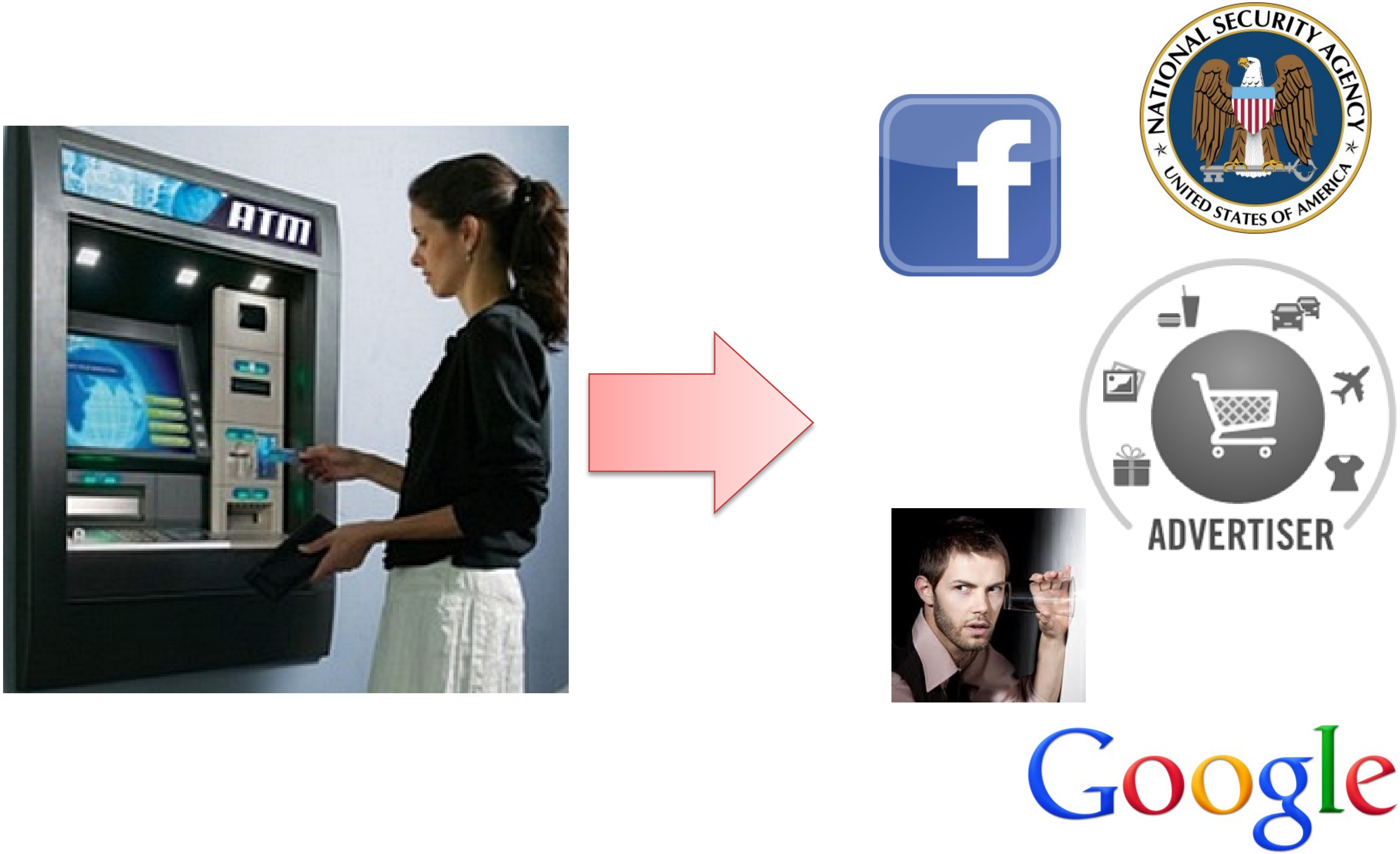
Attack Sophistication vs. Intruder Technical Knowledge



Where was the information stored?

Who had control over the information?

Who valued the information?



Who created the information?

Step-By-Step / Checklist / Roadmap …..

- □
- □ Identify your critical products and services (Why do you exist?)
- □ What dose operational stress mean to you?
- □ Internal environmental scan (What has changed internally?)
- □ External environmental scan (What has changed externally?)
- □ Characterize your risk environment
- □
- □

Operational Resilience

Risk & Resilience

Enterprise Risk Management

Operational Risk Management

Hurdles to effective operational risk management

risk *noun* [risk]

The possibility of suffering harm or loss

Exposure to the chance of injury or loss

A source of danger

The possibility of suffering a harmful event

lawyer): approaching

sloping upwards; ~ butt or

opens). [f. RISE¹ + -ING²]

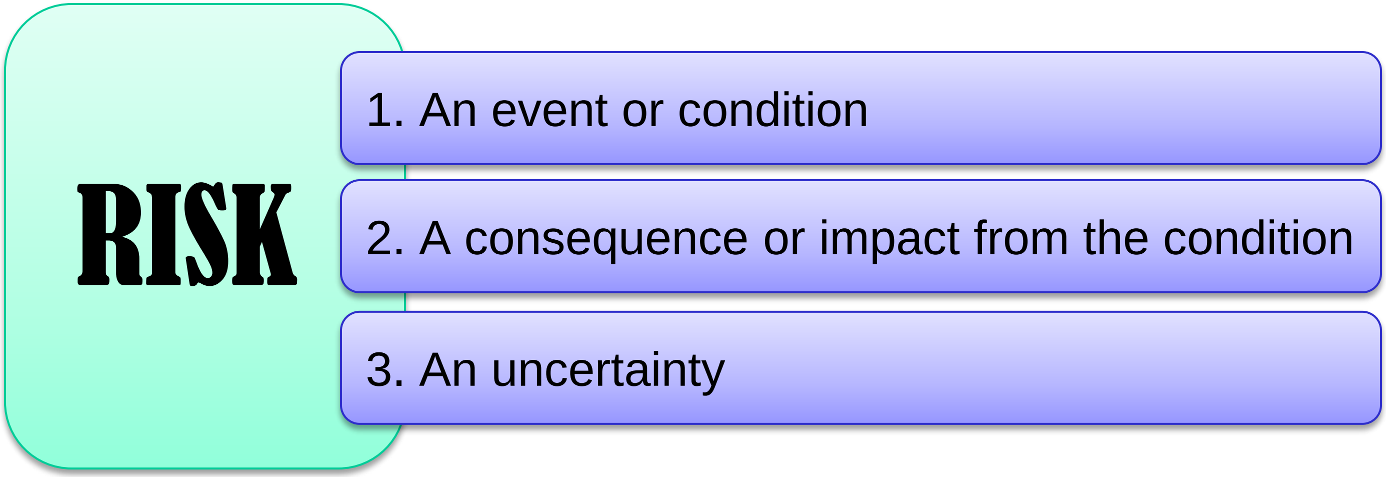
risk *n.*, & *v.t.* **1.** *n.* hazar

consequences, loss, etc., expo

is the risk of his catching cold; a

exposed to danger; **at** perso

any loss etc. resulting; **put**



RISK

1. An event or condition

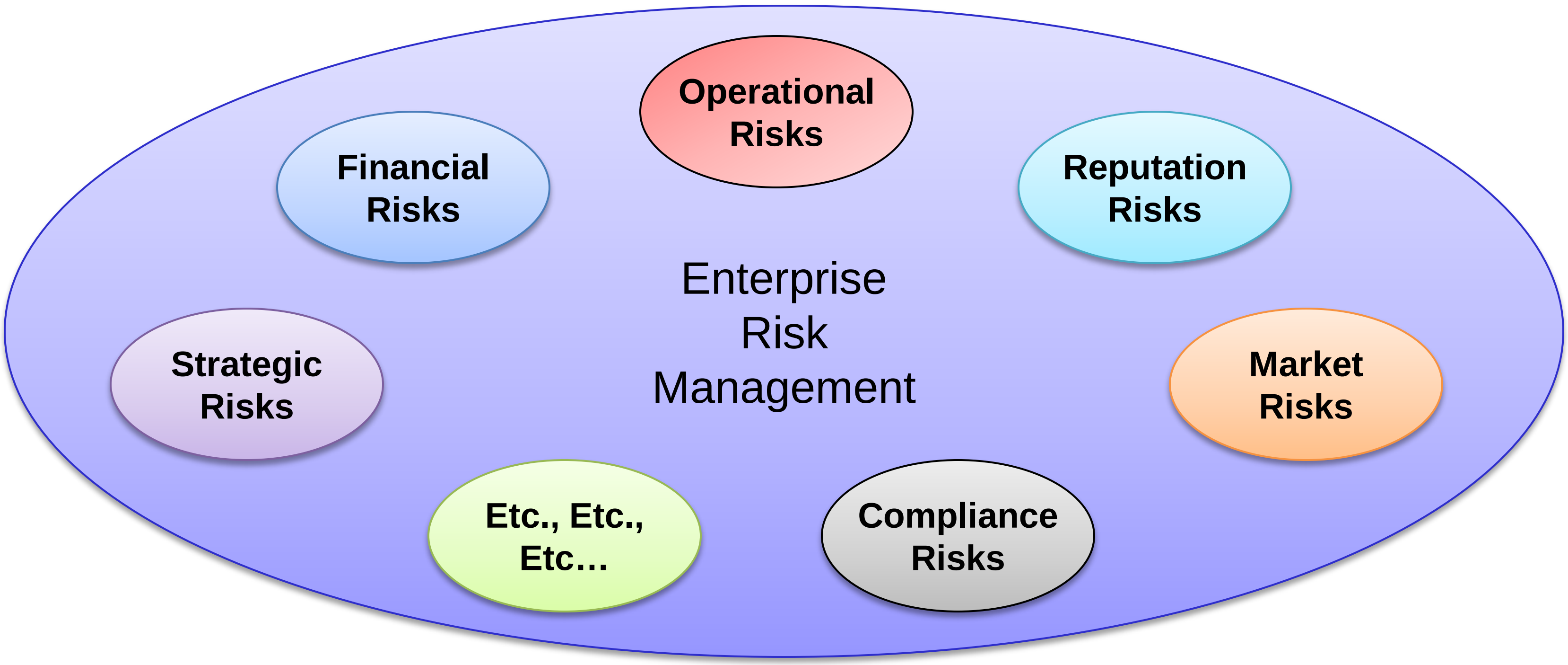
2. A consequence or impact from the condition

3. An uncertainty

Enterprise Risk Management

Looks across all types of risk activities in the organization and considers all types of risks

Connects risk management to strategic and business drivers



Operational Risk

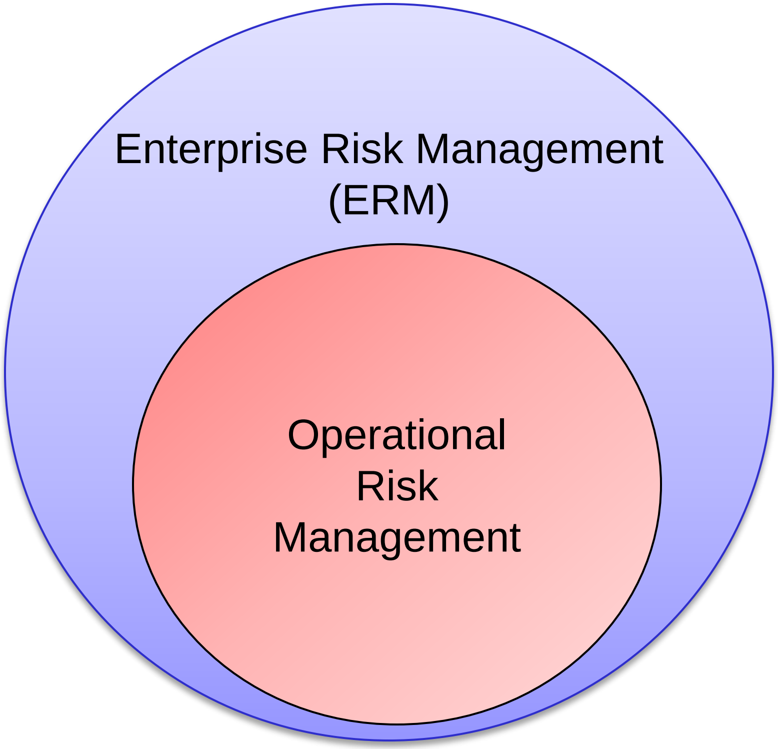
A form of risk affecting day-to-day business operations

A very broad risk category

- from high-frequency low-impact to low-frequency high-impact

Exacerbated by

- actions of people
- systems and technology failures
- failed internal processes
- external events



Actions of People

Inadvertent or deliberate

Direct or indirect

Mistakes, errors, omissions

Deliberate actions such as insider threat, sabotage, fraud

Lack of skills or knowledge

Lack of availability

Poor leadership or guidance

Poor governance

Lack of training & education

Etc., Etc., Etc…

Systems and Technology Failures

Lack of proper system maintenance

Poor configuration and change management

Insecure, inefficient, or complex coding

Lack of testing and remediation

Poor software and systems engineering practices

Interface failures

Inadequate testing in relevant operational environments

Etc., Etc., Etc…

Failed Internal Processes

Poor process design and execution

Mistakes, errors, omissions

Poor supply chain management

Poor product development

Poor capacity planning

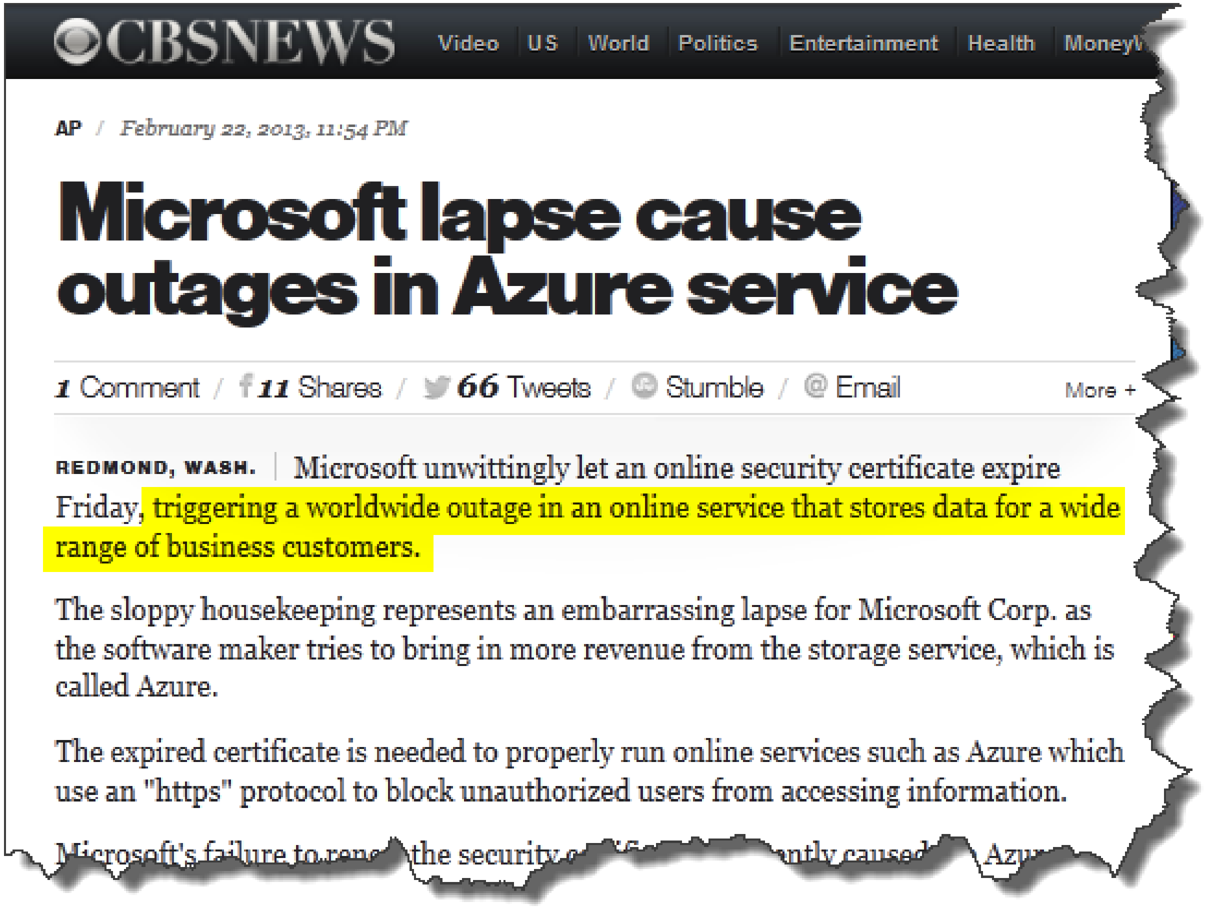
Lack of process controls

Poor support processes (e.g., accounting, HR, education & training, risk management)

Poor governance and compliance

Etc., Etc., Etc…

Failed Internal Processes



AP / February 22, 2013, 11:54 PM

Microsoft lapse cause outages in Azure service

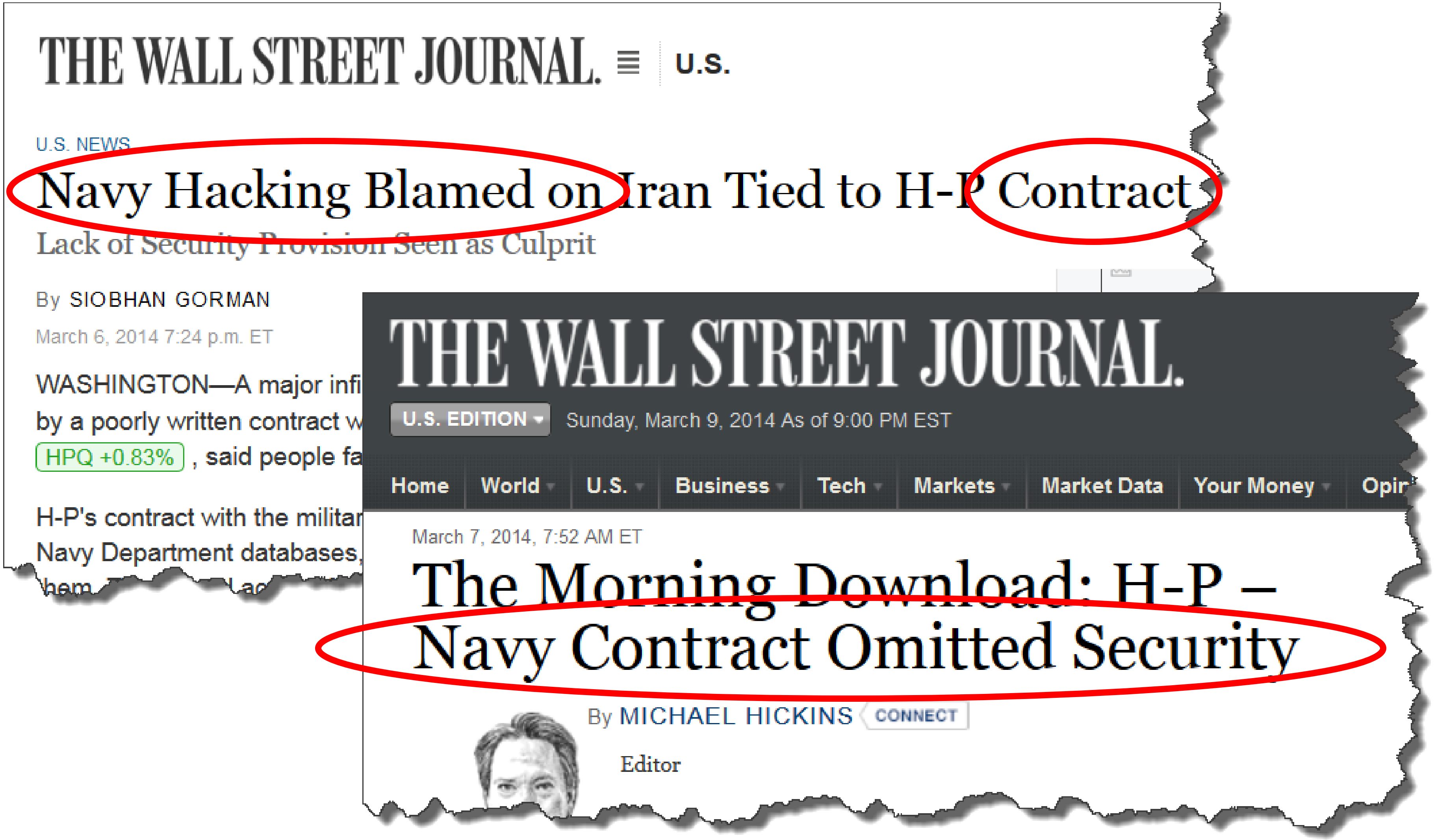
REDMOND, WASH. Microsoft unwittingly let an online security certificate expire Friday, triggering a worldwide outage in an online service that stores data for a wide range of business customers.

The sloppy housekeeping represents an embarrassing lapse for Microsoft Corp. as the software maker tries to bring in more revenue from the storage service, which is called Azure.

The expired certificate is needed to properly run online services such as Azure which use an "https" protocol to block unauthorized users from accessing information.

Microsoft's failure to rene the security c ntly caused Azu

Failed Internal Processes – March 6, 2014



THE WALL STREET JOURNAL. ≡ U.S.

U.S. NEWS

Navy Hacking Blamed on Iran Tied to H-P Contract

Lack of Security Provision Seen as Culprit

By SIOBHAN GORMAN

March 6, 2014 7:24 p.m. ET

WASHINGTON—A major infi

by a poorly written contract w

HPQ +0.83% , said people fa

H-P's contract with the militar

Navy Department databases,

THE WALL STREET JOURNAL.

Sunday, March 9, 2014 As of 9:00 PM EST

March 7, 2014, 7:52 AM ET

The Morning Download: H-P – Navy Contract Omitted Security

By MICHAEL HICKINS

Editor

External Events

Natural disasters (e.g., hurricane, earthquake, flood, disease, volcano)

Terrorism

Supply chain failures

Boycotts

Economic pressures

Political pressures

Outsourcing

Business cycles

Wars

Etc., Etc., Etc…

Why do operational risks matter?

Trust and confidence of employees and customers

Reputation and image

Regulatory compliance, fines, and legal penalties

Customer retention and growth

Life, safety, and health of customers and employees

Productivity and profitability

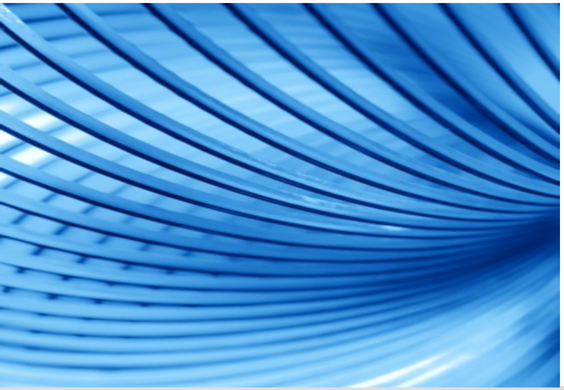
Organizational survival

… because they have explicit and direct IMPACT

Step-By-Step / Checklist / Roadmap …..

- ❑
- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment
- ❑ What are your operational risks? Who will be affected if there are realized?

Concept of Resilience
&
Operational Resilience



A Tree under Operational Stress…

…while achieving its “business” mission

re·sil·ience *noun* [ri-ˈzil-yəns]

power or ability to return to the original form, position, etc. after being bent, compressed, or stretched

ability of an ecosystem to return to its original state after being disturbed

ability to recover from or adjust easily to misfortune or change

physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit

ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation

ability to recover readily from illness, depression, adversity, or the like

capability of a strained body to recover its size and shape after deformation

Operational Resilience

The ***emergent*** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated

Operational Resilience

The ***emergent*** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated

- Organization
- Nation
- Armed Forces
- Critical Infrastructure
- System
- Network
- Supply Chain
- Community
- An Ecosystem
- Cyberspace

An Analogy: Health

Is there a place that you can purchase health?

Is there a place where health is manufactured?

How do you become healthy?

Health & Resilience: They are both emergent properties.

Operational resilience and operational risk

Operational resilience emerges from effective **operational risk management**

Operational risk categories:

Actions of people

```
A fatal exception
000059F8. The curr
* Press any key to
* Press CTRL+ALT+D
  lose any unsaved
```

Systems and technology failures

Failed internal processes

External events

What makes an entity operationally resilient?

Operational Resilience is an emergent property;

It emerges from things that we do, like these:

dentification and mitigation of risks to ervice and related assets

Se ontinuity processes and plann

Manageme T operations practices

Management a ployment of people

Practices to protect ol) and secure important information chnology assets

Management of external part hat provide parts of the service)

Environmental management (where t service “lives”)

… a long list of good things to do on a regular basis.

Operational Resilience Management

It is the overarching (risk management) practice of planning, developing, integrating, executing, and governing activities to ensure that an entity and the environment that it operates in are able to:

- Identify and mitigate operational risks that can lead to system disruptions before they occur,
- Prepare for and respond to disruptive events (natural or man-made, accidental or intentional) in a manner that demonstrates command and control of incident response, and
- Recover and restore mission-critical operations following a disruptive event within acceptable time frames.

Hurdles to Effective Operational Resilience Management

Vague and abstract nature

Compartmentalization

Technology focus

Practice proliferation

Insufficient funding

Insufficient success metrics

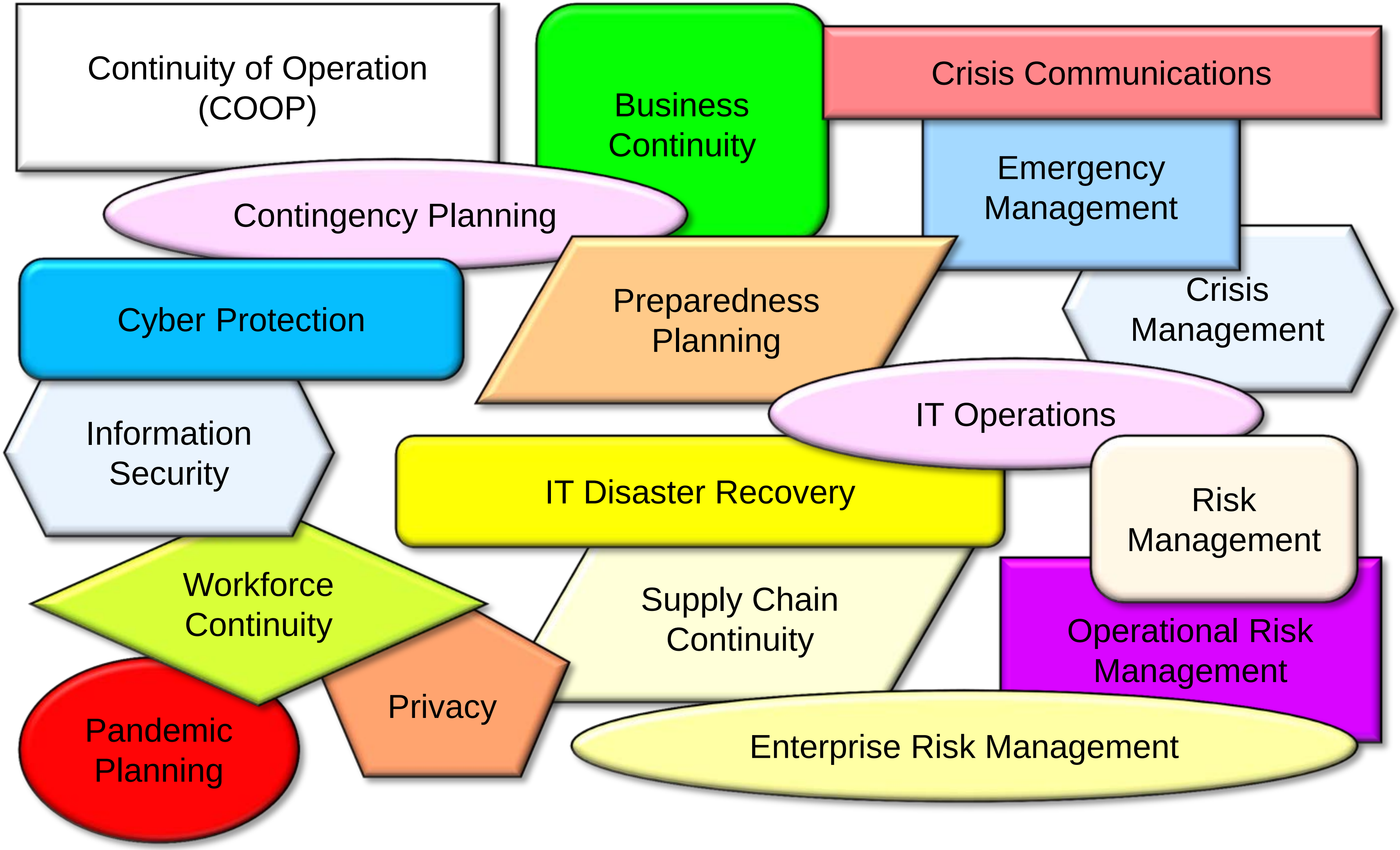
Discrete nature of activity

(Over)reliance on people

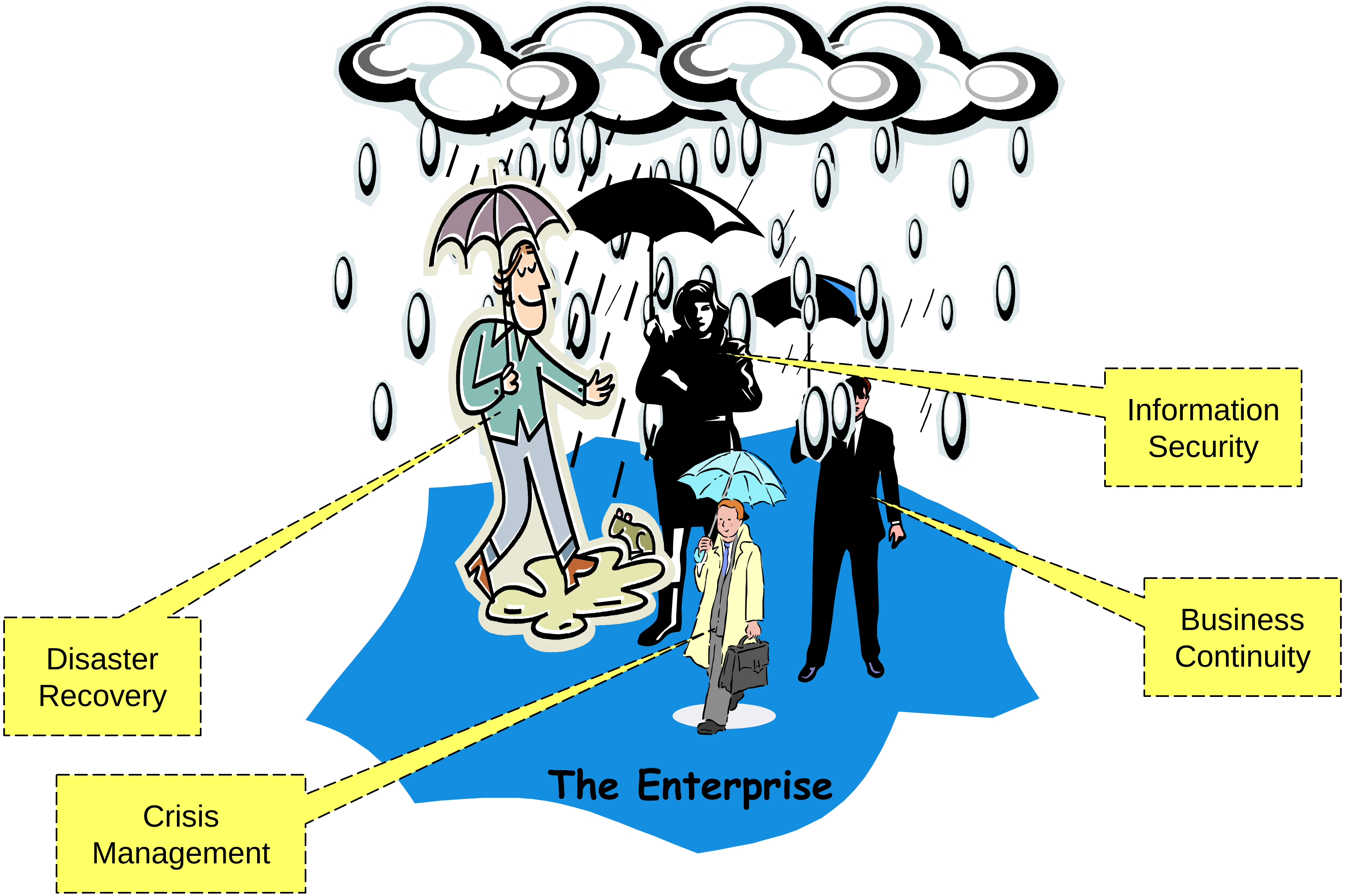
Regulatory climate

Head-in-the-sand

Multiplicity of Preparedness Planning Efforts



Another Analogy



Step-By-Step / Checklist / Roadmap …..

❑

❑ Identify your critical products and services (Why do you exist?)

❑ What dose operational stress mean to you?

❑ Internal environmental scan (What has changed internally?)

❑ External environmental scan (What has changed externally?)

❑ Characterize your risk environment.

❑ What are your operational risks? Who will be affected if there are realized?

❑ What hurdles do you face to effective operational resilience management?

Cornerstones of Operational Resilience

Cornerstones of Operational Resilience

- Risk Management
  - Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities
- Protection and Sustainment Activities
- Lifecycle View
- Institutionalization

Operational Risk Management

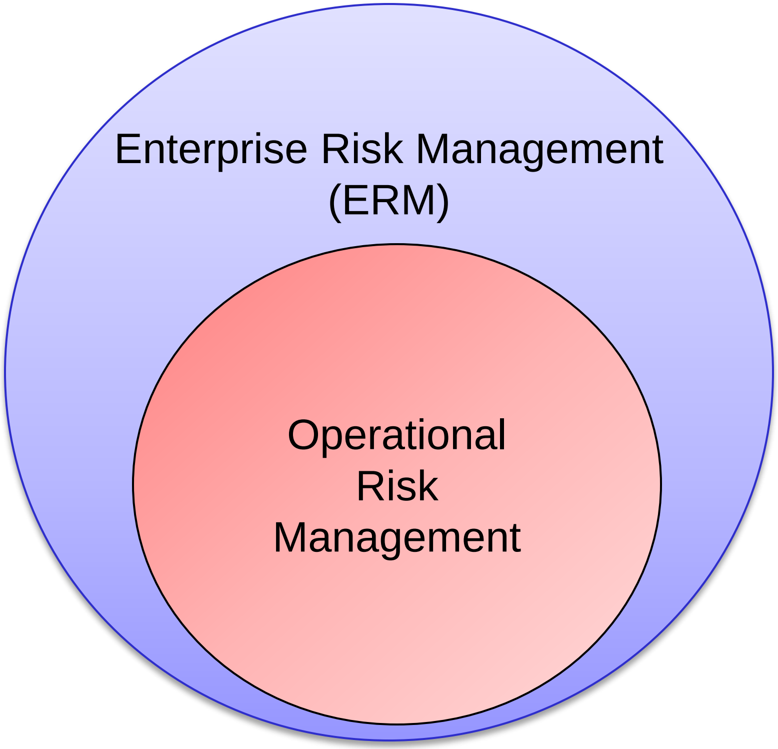
A form of risk affecting day-to-day business operations

A very broad risk category

- From high-frequency low-impact to low-frequency high-impact

Exacerbated by

- Actions of people
- Systems and technology failures
- Failed internal processes
- External events



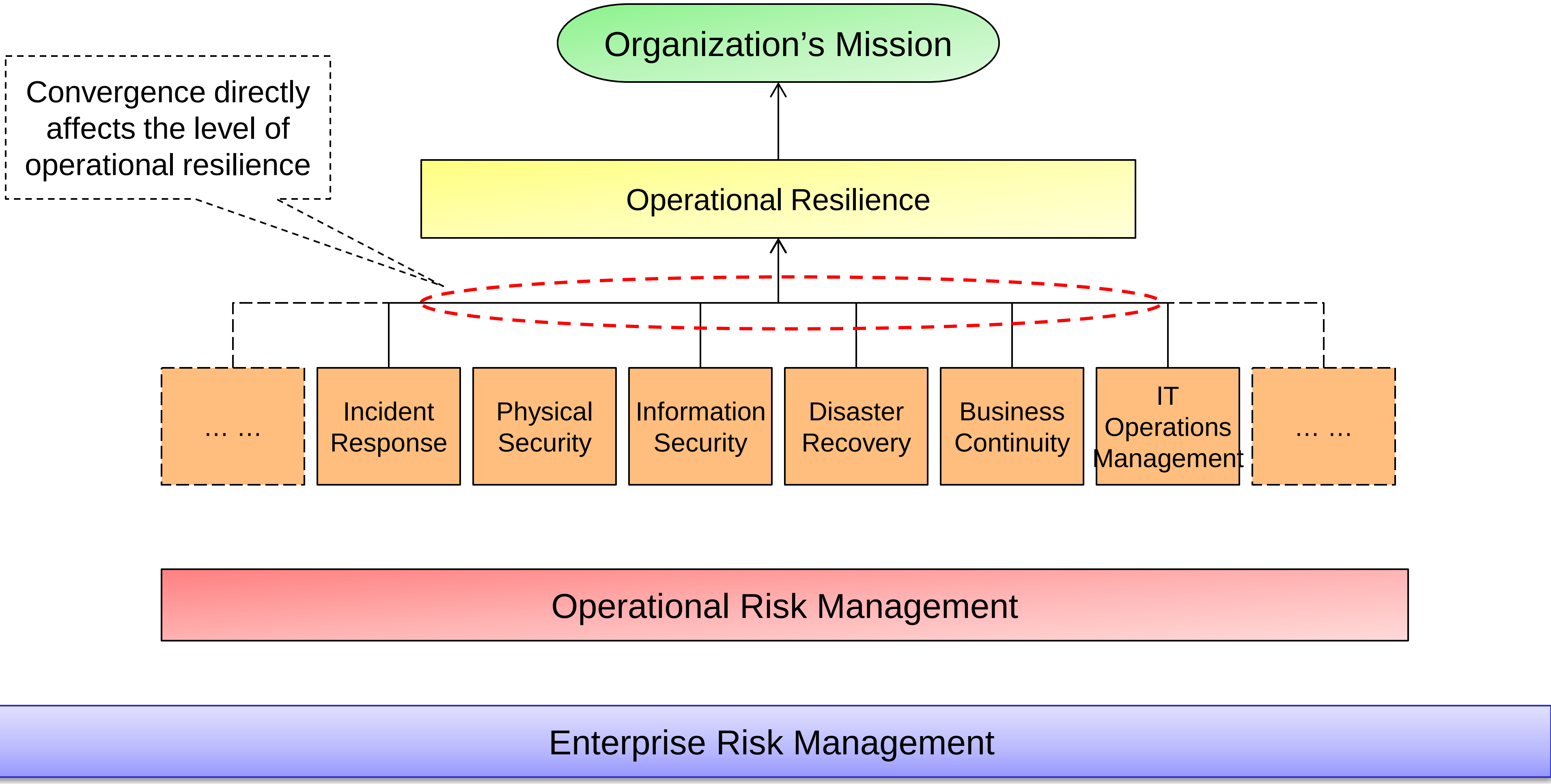
Operational resilience emerges from effective management of operational risk.

Cornerstones of Operational Resilience

✓ Risk Management
  - Operational Risk Management

- Convergence
- Organizational Construct for Resilience Activities
- Protection and Sustainment Activities
- Lifecycle View
- Institutionalization

Convergence



Convergence directly affects the level of operational resilience

Organization's Mission

Operational Resilience

… …

Incident Response

Physical Security

Information Security

Disaster Recovery

Business Continuity

IT Operations Management

… …

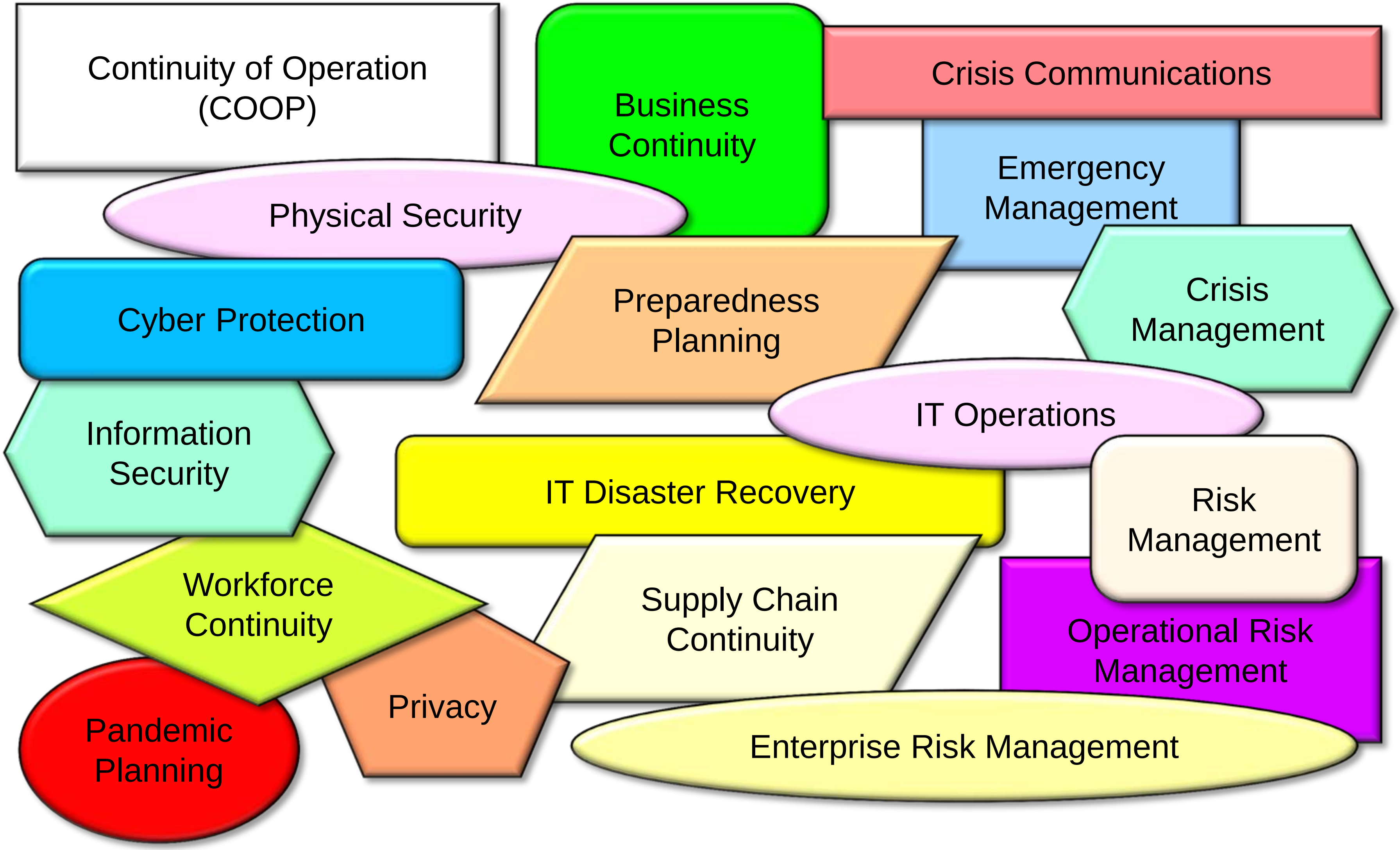
Operational Risk Management

Enterprise Risk Management

Benefits of Convergence and Integration

- Similar activities are bound by same risk drivers
- Allows for better alignment between risk-based activities and organizational risk tolerances and appetite
- Eliminates redundant activities (and associated costs)
- Forces collaboration between activities that have similar objectives
- Enforces a mission focus
- Facilitates a process that is owned across the organization
- Influences how operational risk and resilience management work is planned, executed, and managed

Multiplicity of Preparedness Planning Efforts



Continuity of Operation (COOP)

Business Continuity

Crisis Communications

Emergency Management

Physical Security

Cyber Protection

Preparedness Planning

Crisis Management

IT Operations

Information Security

IT Disaster Recovery

Risk Management

Workforce Continuity

Supply Chain Continuity

Operational Risk Management

Privacy

Pandemic Planning

Enterprise Risk Management

An Analogy

Chief Information Officer

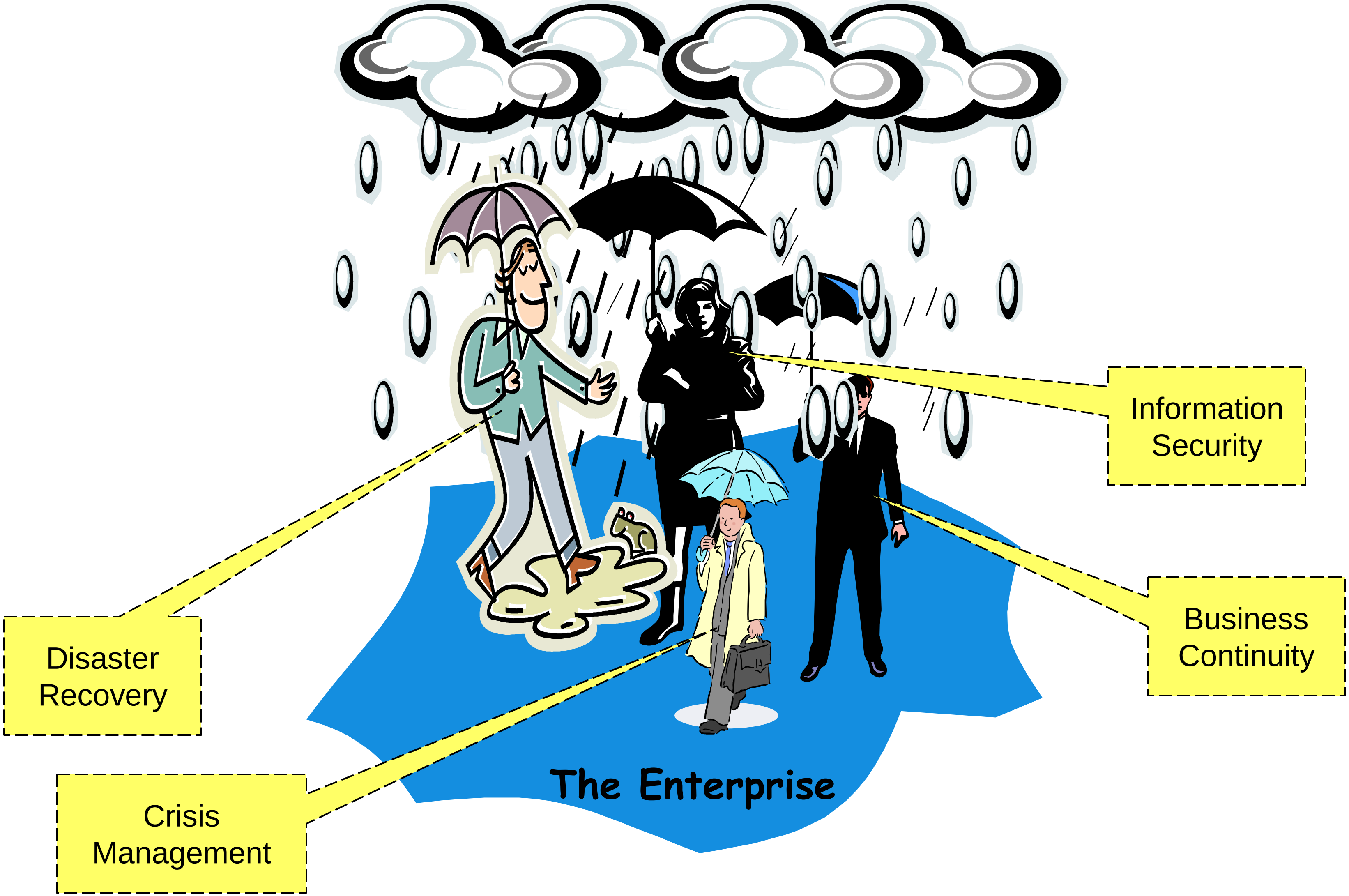
Chief Information Security Officer

Human Resources Department

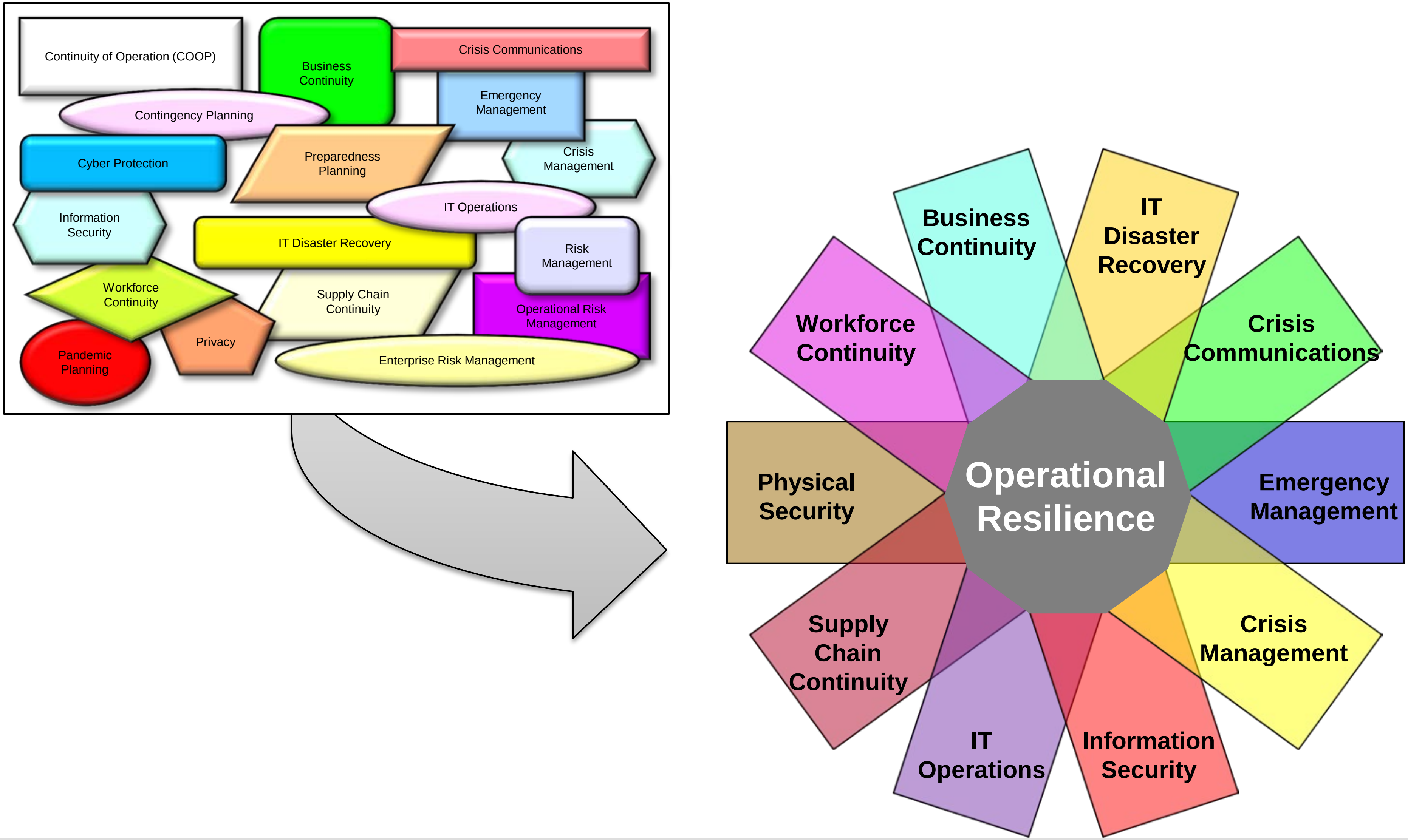
Corporate Communications

Corporate Security

Another Analogy



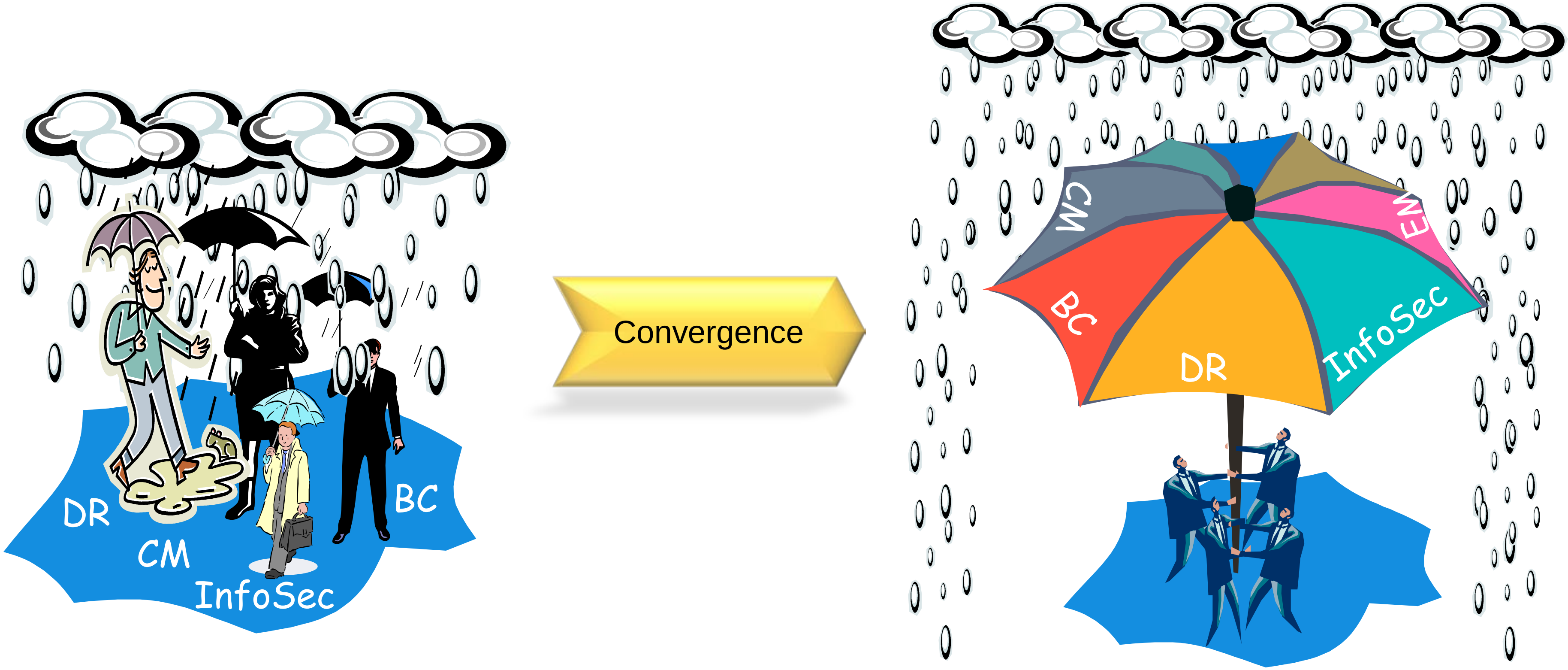
Desired Solution Approach



Continuity of Operation (COOP)
Business Continuity
Crisis Communications
Emergency Management
Contingency Planning
Cyber Protection
Preparedness Planning
Crisis Management
IT Operations
Information Security
IT Disaster Recovery
Risk Management
Workforce Continuity
Supply Chain Continuity
Operational Risk Management
Privacy
Pandemic Planning
Enterprise Risk Management

Operational Resilience
Business Continuity
IT Disaster Recovery
Workforce Continuity
Crisis Communications
Physical Security
Emergency Management
Supply Chain Continuity
Crisis Management
IT Operations
Information Security

Desired Solution Approach: An Analogy



Convergence

Enemies of convergence

- Organizational structures
- Traditional funding models
- Overuse and misuse of codes of practice
- Unclear or poorly defined and communicated risk drivers
- Unclear or poorly defined enterprise objectives, strategic objectives, and critical success factors
- Lack of supporting process-orientation and definition
- Lack of sponsorship and governance for the process
- Lack of a risk-aware culture

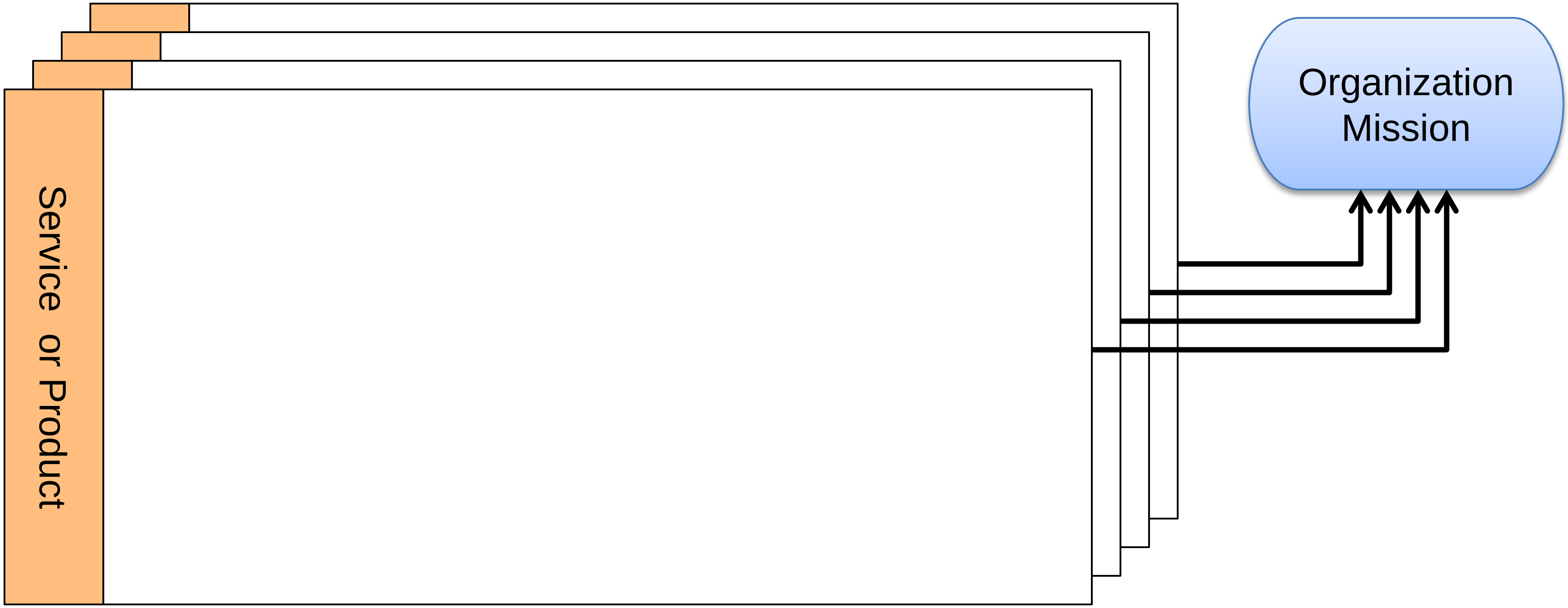
Step-By-Step / Checklist / Roadmap …..

- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment.
- ❑ What are your operational risks? Who will be affected if there are realized?
- ❑ What hurdles do you face to effective operational resilience management?
- ❑ What operational risk management activates (silos) exist? Are there opportunities for convergence of some sort? Where would you start?

Cornerstones of Operational Resilience

- ✓ Risk Management
  - Operational Risk Management
- ✓ Convergence
- Organizational Construct for Resilience Activities
- Protection and Sustainment Activities
- Lifecycle View
- Institutionalization

Services and Products

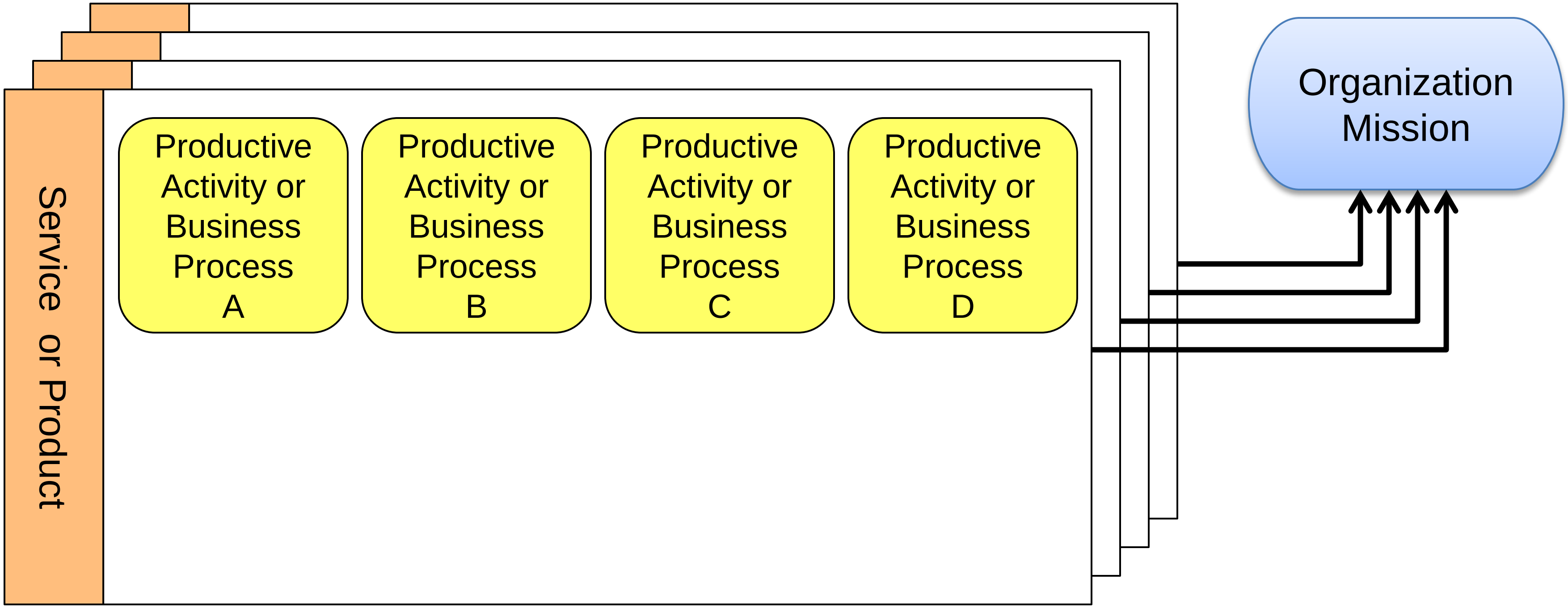


Outputs of an organization

can be internally or externally focused.

Collectively they enable an organization’s mission.

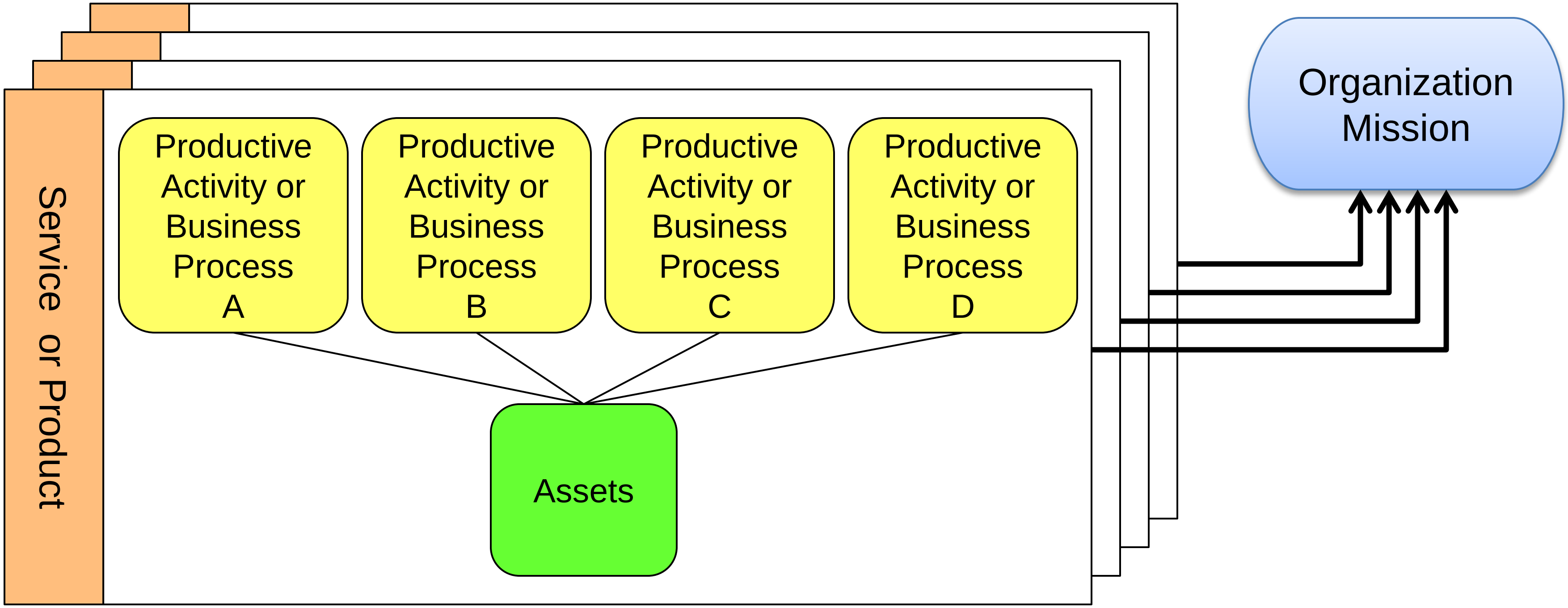
Productive Activities or Business Processes


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
Organization Mission

Activities that the organization (and/or its suppliers) perform to ensure that services and products are generated

A service or product is made up of one or more business processes.

Assets


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
Assets
Organization Mission

Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.

Asset Types of Importance to Operational Resilience

People

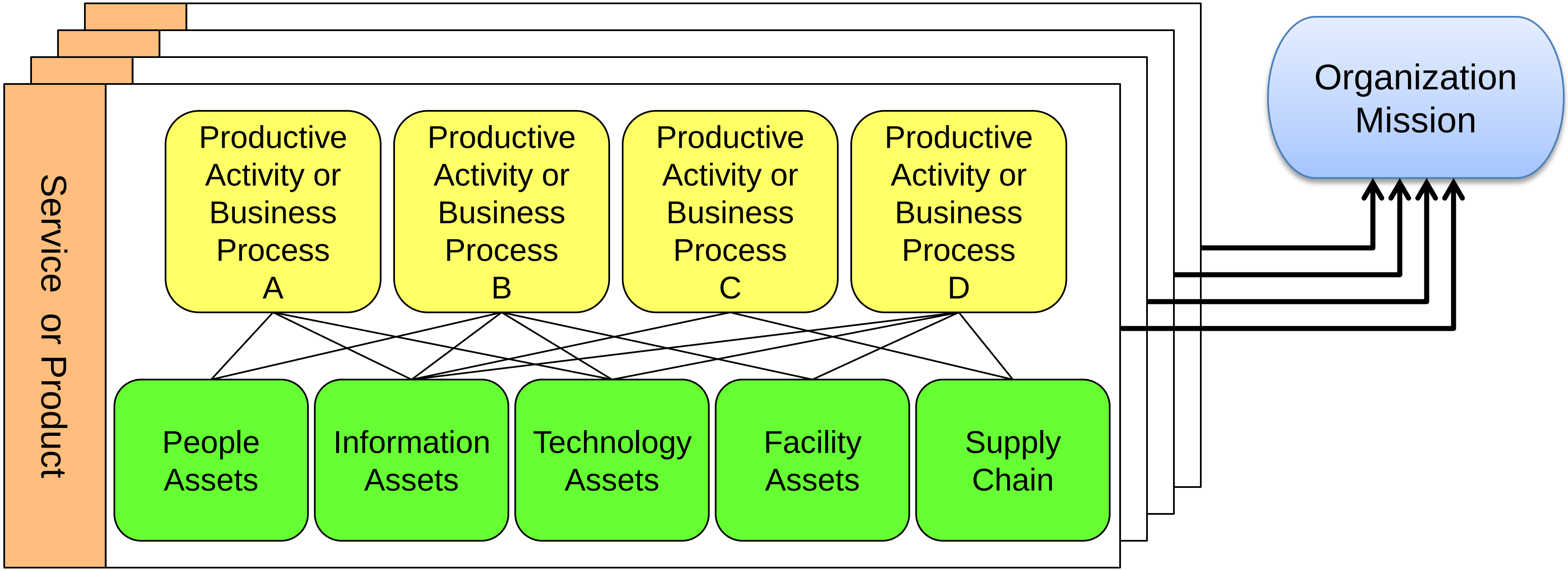
Information

Facilities

Technology

Supply Chain / Raw Material

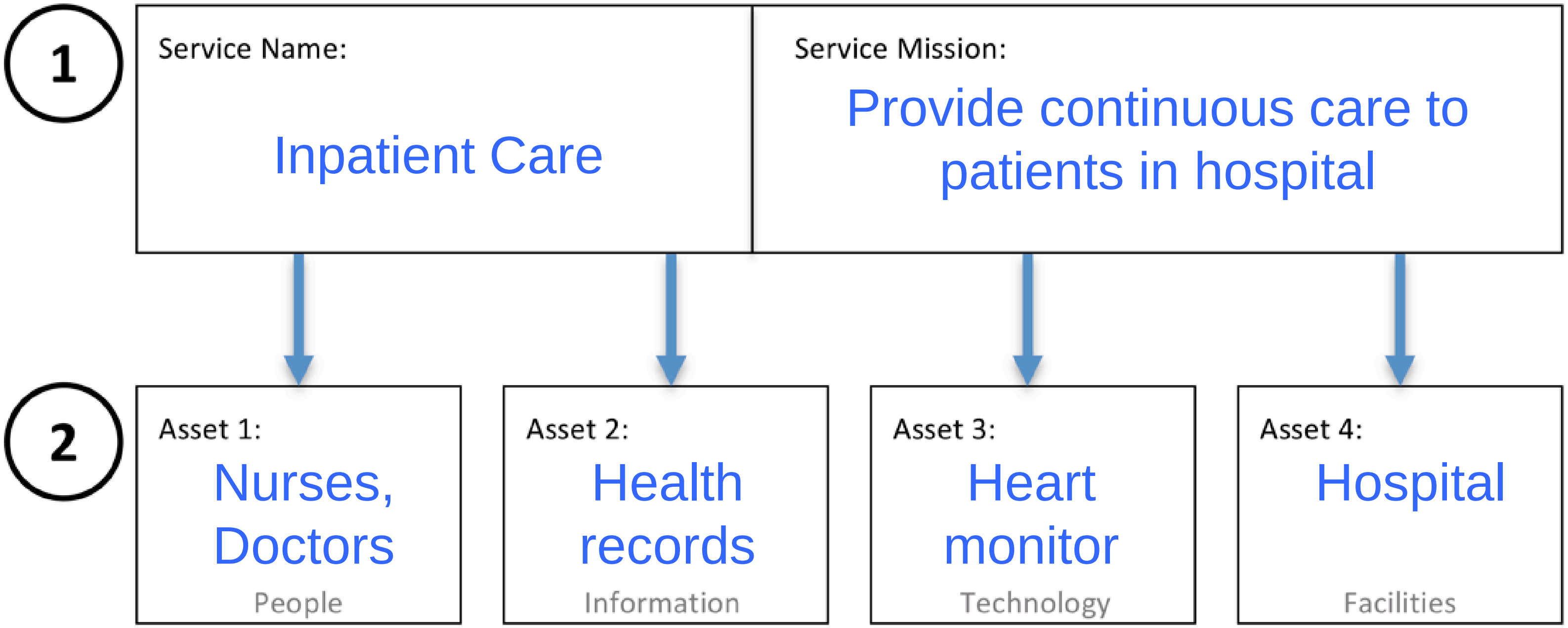
Asset Types


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Organization Mission

Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.

Exercise - Steps 1 & 2



1

Service Name:

Inpatient Care

Service Mission:

Provide continuous care to patients in hospital

2

Asset 1:

Nurses, Doctors

People

Asset 2:

Health records

Information

Asset 3:

Heart monitor

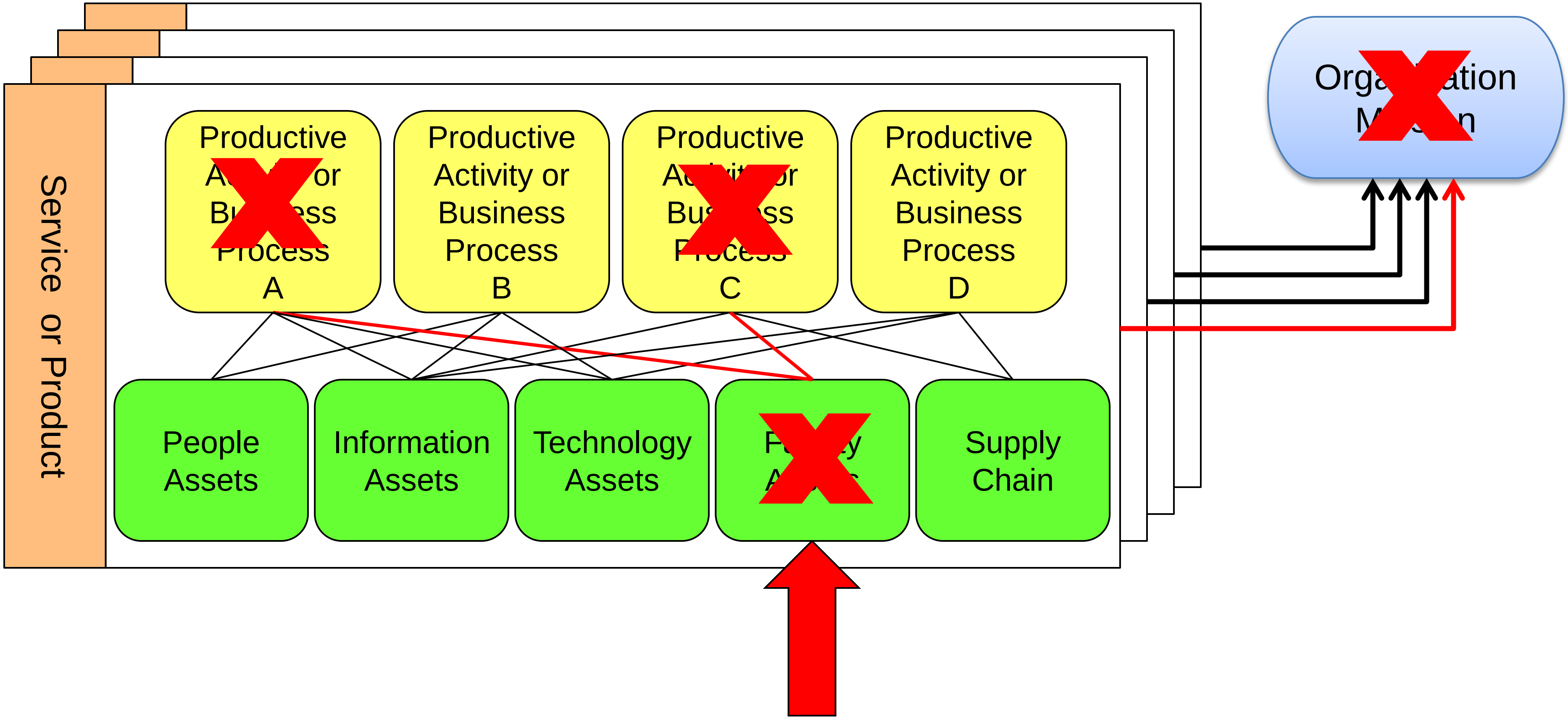
Technology

Asset 4:

Hospital

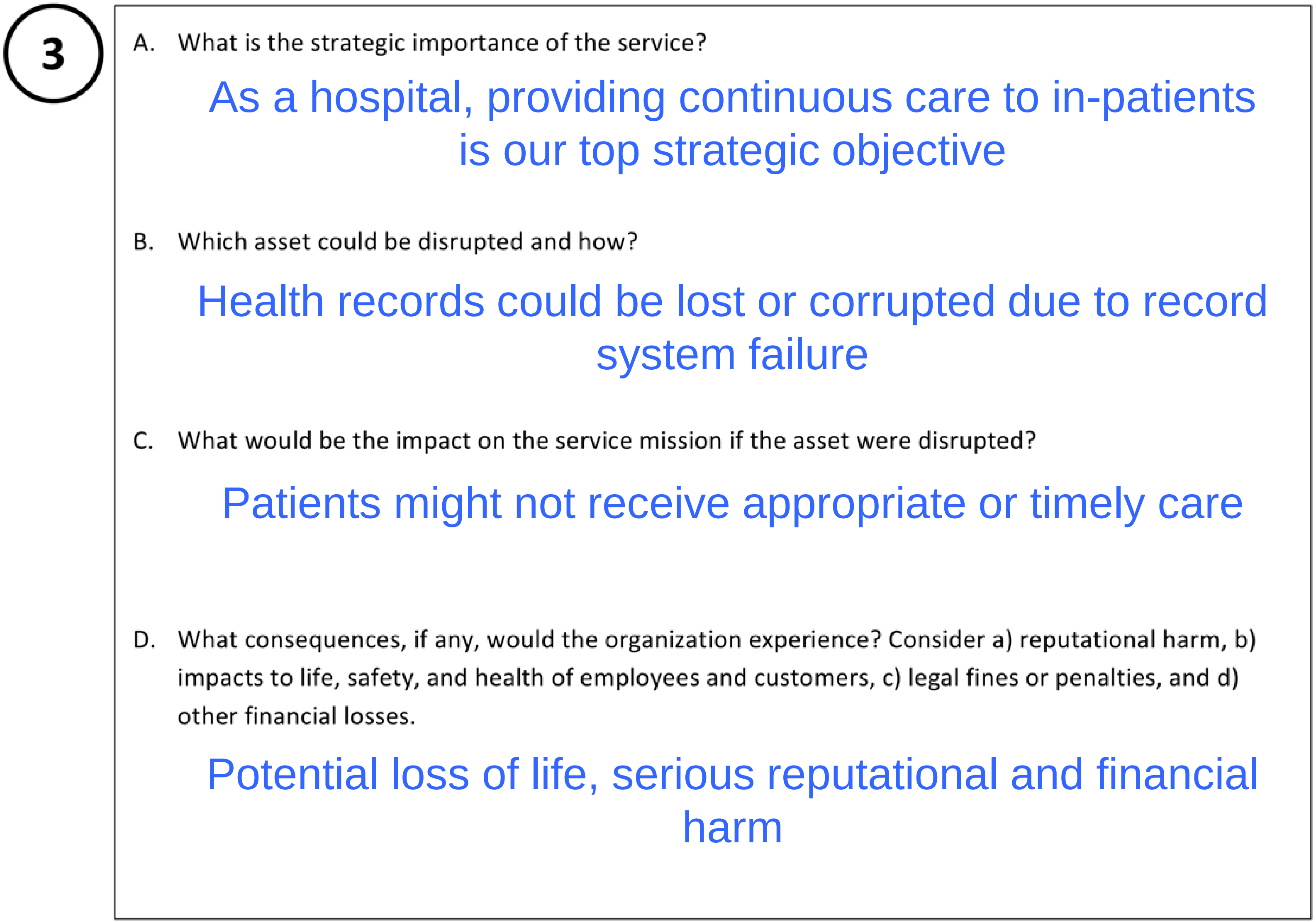
Facilities

Operational Resilience Starts at Asset Level


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Organization Mission

Realized operational risk resulting in asset disruption

Exercise - Step 3



3

A. What is the strategic importance of the service?

As a hospital, providing continuous care to in-patients is our top strategic objective

B. Which asset could be disrupted and how?

Health records could be lost or corrupted due to record system failure

C. What would be the impact on the service mission if the asset were disrupted?

Patients might not receive appropriate or timely care

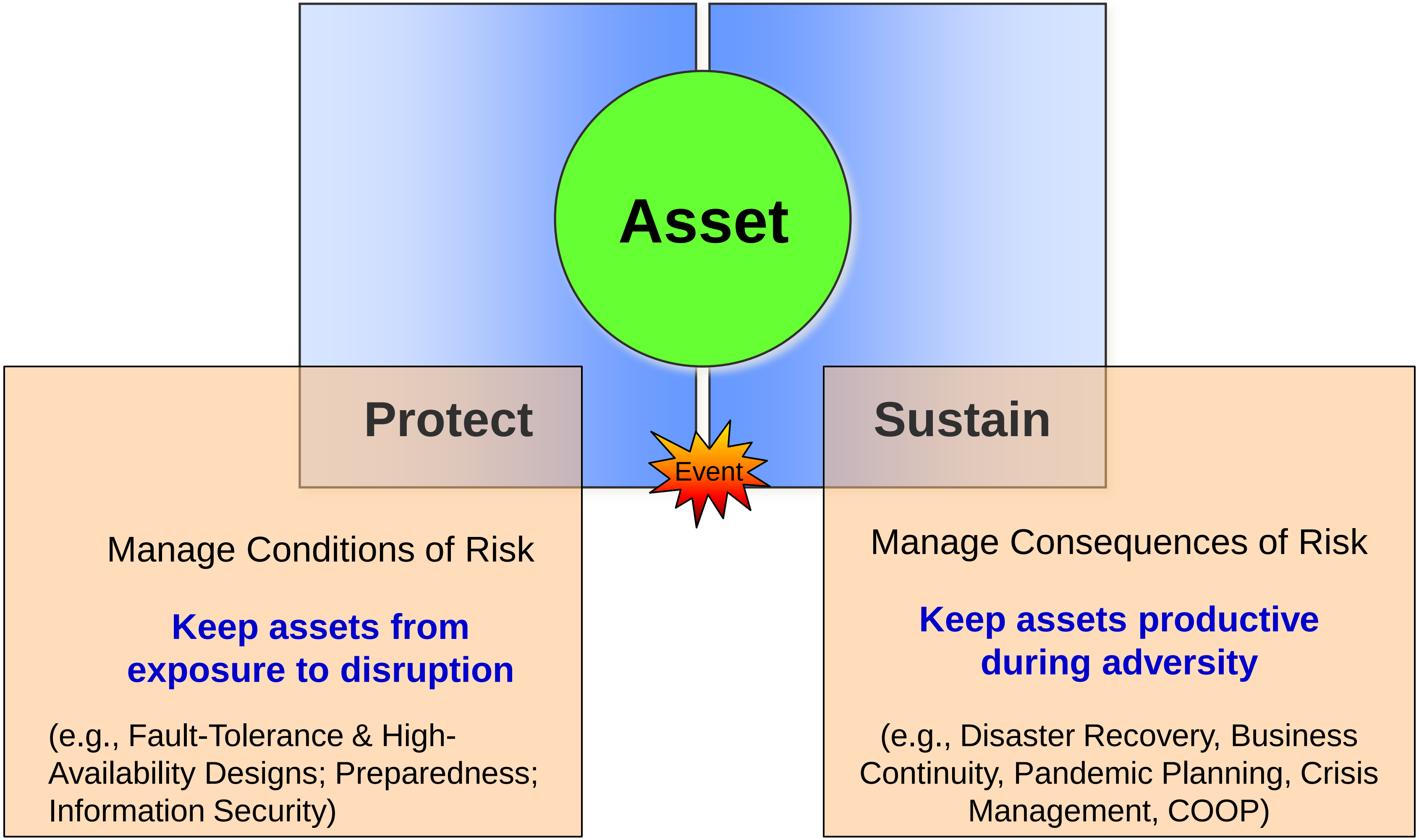
D. What consequences, if any, would the organization experience? Consider a) reputational harm, b) impacts to life, safety, and health of employees and customers, c) legal fines or penalties, and d) other financial losses.

Potential loss of life, serious reputational and financial harm

Cornerstones of Operational Resilience

- ✓ Risk Management
  - Operational Risk Management
- ✓ Convergence
- ✓ Organizational Construct for Resilience Activities
- Protection and Sustainment Activities
- Lifecycle View
- Institutionalization

Operational Resilience Starts at Asset Level



Asset

Protect

Event

Sustain

Manage Conditions of Risk

Keep assets from exposure to disruption

(e.g., Fault-Tolerance & High-Availability Designs; Preparedness; Information Security)

Manage Consequences of Risk

Keep assets productive during adversity

(e.g., Disaster Recovery, Business Continuity, Pandemic Planning, Crisis Management, COOP)

Analogy - Protection and Sustainment Strategies

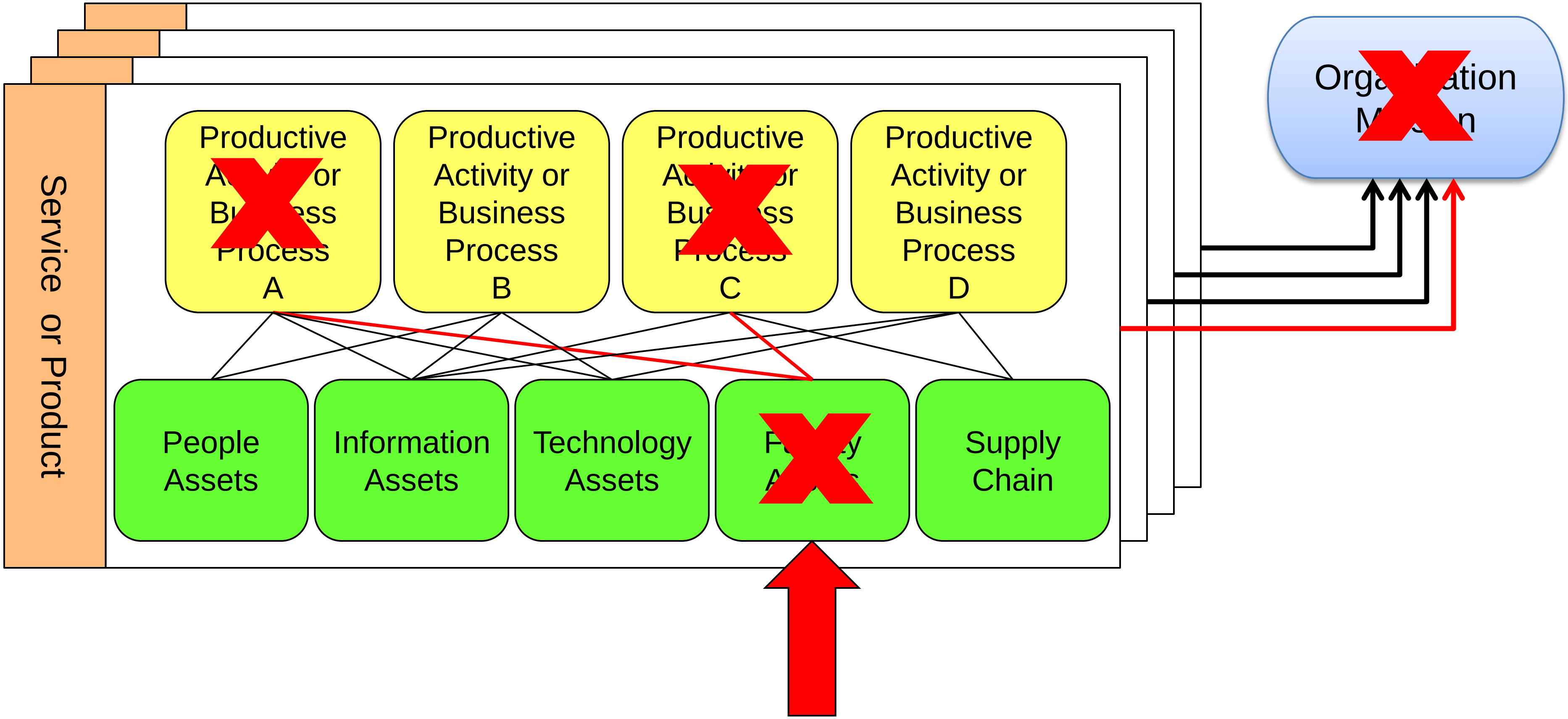
Protection Activities

- Translate into activities designed to keep assets from exposure to disruption
- Example: “security” activities, but may also be embedded in IT operations activities

Sustainability Activities

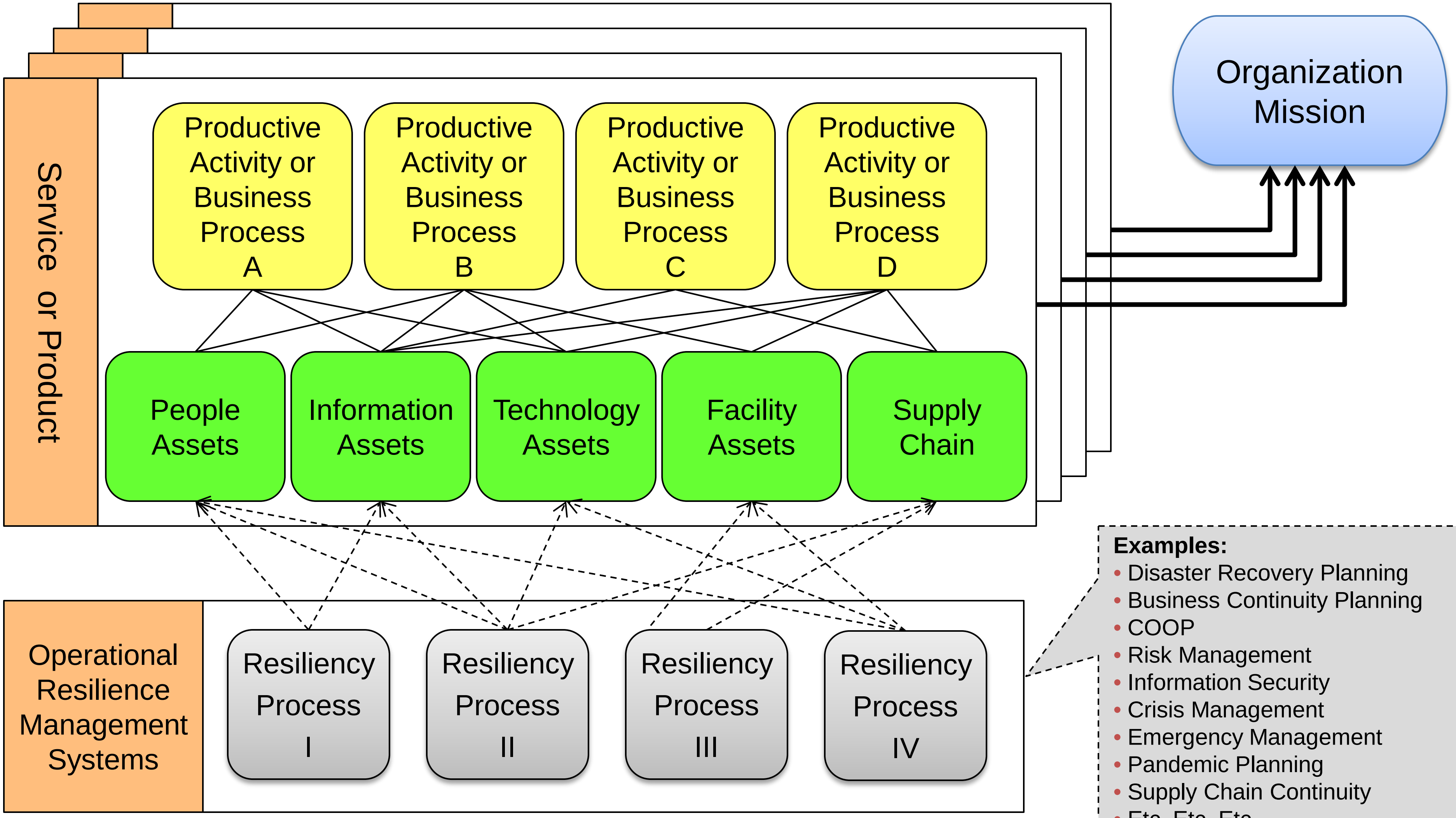
- Translate into activities designed to keep assets productive during adversity
- Example: “business continuity” activities

Asset Disruption


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Organization Mission

Realized operational risk resulting in asset disruption

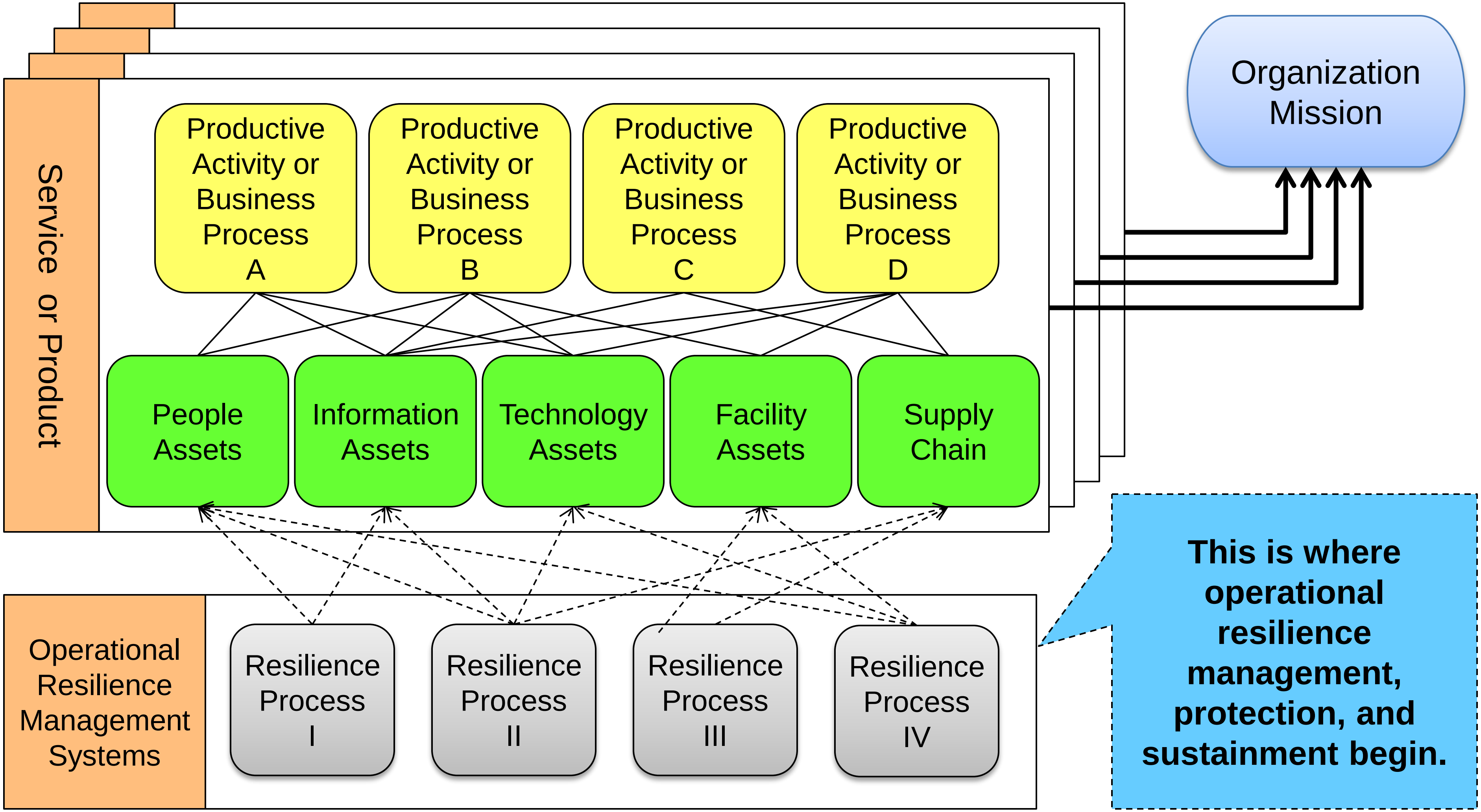
Organizational Context for Resiliency Activities


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Organization Mission
Operational Resilience Management Systems
Resiliency Process I
Resiliency Process II
Resiliency Process III
Resiliency Process IV

Examples:

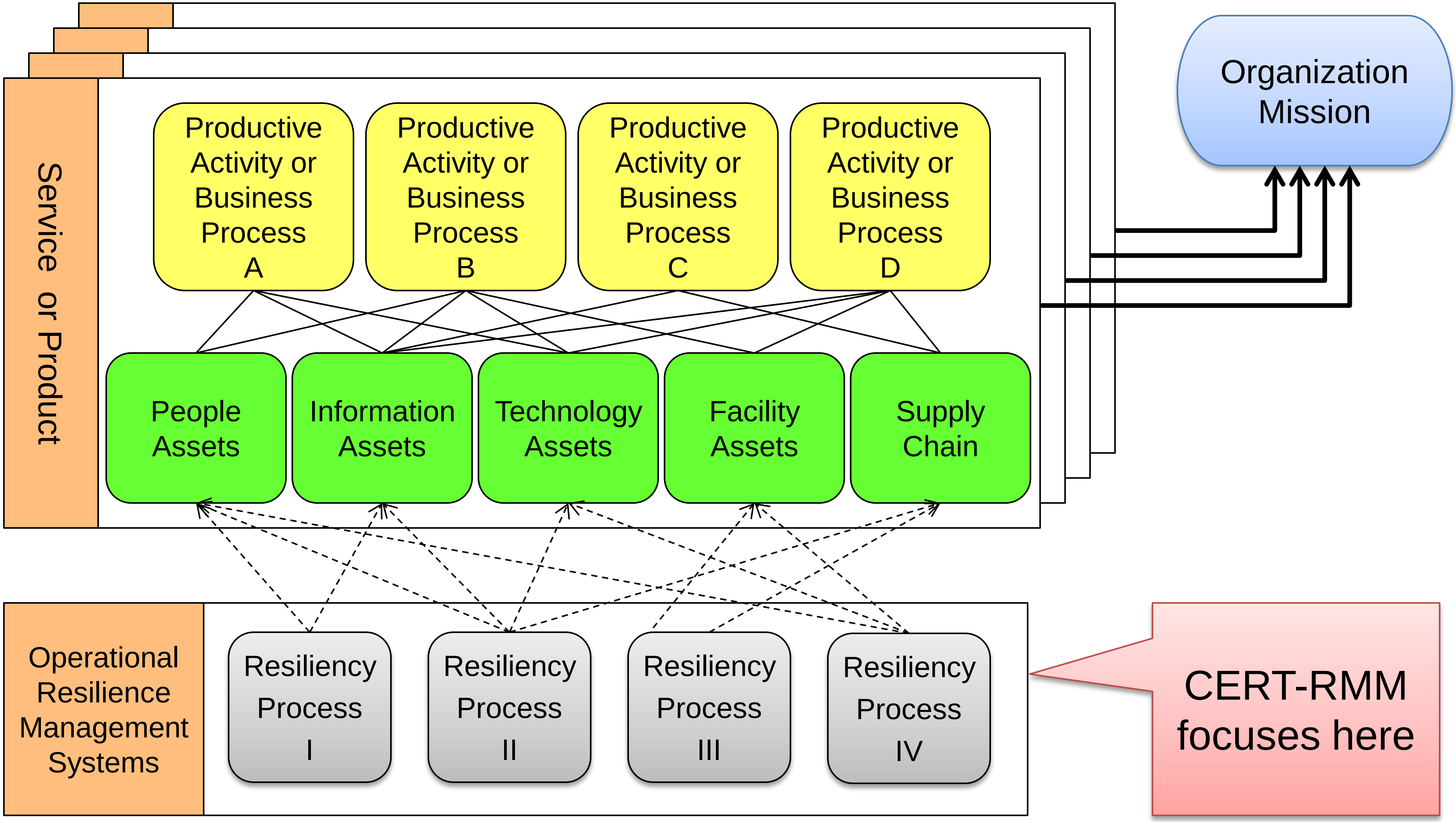
- Disaster Recovery Planning
- Business Continuity Planning
- COOP
- Risk Management
- Information Security
- Crisis Management
- Emergency Management
- Pandemic Planning
- Supply Chain Continuity
- Etc, Etc, Etc…

Organizational Context for Resilience Activities


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Organization Mission
Operational Resilience Management Systems
Resilience Process I
Resilience Process II
Resilience Process III
Resilience Process IV

This is where operational resilience management, protection, and sustainment begin.

Organizational Context for Resiliency Activities


Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Organization Mission
Operational Resilience Management Systems
Resiliency Process I
Resiliency Process II
Resiliency Process III
Resiliency Process IV

CERT-RMM focuses here

Step-By-Step / Checklist / Roadmap …..

- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment.
- ❑ What are your operational risks? Who will be affected if there are realized?
- ❑ What hurdles do you face to effective operational resilience management?
- ❑ What operational risk management activates (silos) exist? Are there opportunities for convergence of some sort? Where would you start?
- ❑ Draw the resilience context diagram for your organization.

Resilience Requirements Drive Strategies

Resilience requirement

- A constraint that the organization places on the productive capability of an asset to operational resilience of services to which the asset is associated with

Are the foundation for

- Protection strategies (security controls, etc.)
- Sustainment strategies (service continuity plans, etc.)

Must reflect organization’s risk tolerances and appetite

Levels of requirements

Three levels of resilience requirements

1. **Enterprise** – reflect enterprise-level needs, expectations, and constraints
   - Example: HIPAA privacy regulations

2. **Service** – reflect the resilience needs of a service in pursuit of its mission

3. **Asset** – set by the owners of the assets and establish the asset’s protection and sustainment needs

Iteration may be necessary to harmonize across levels

Types of requirements

Confidentiality – Ensuring that only authorized people, processes, or devices have access to an information asset

Integrity – Ensuring that an asset remains in the condition intended and so continues to be useful for the purposes intended

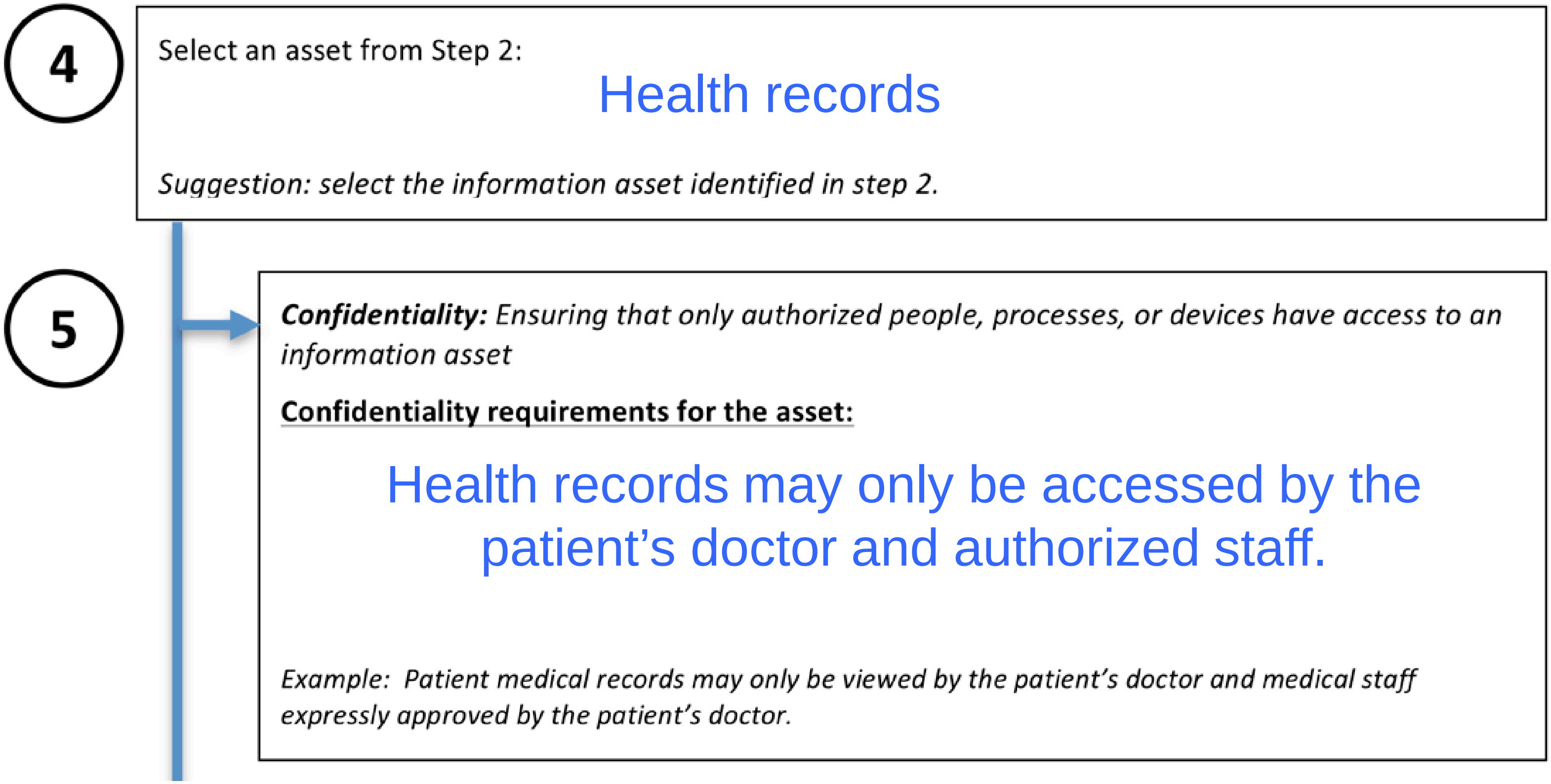
Availability – Ensuring that an asset remains accessible to authorized users (people, processes, or devices) whenever it is needed

Applicability of requirements

Not all resilience requirement types apply to all asset types under all circumstances.

Resilience Requirement	Asset Type			
	People	Information	Technology	Facilities
Confidentiality	--	X	--	--
Integrity	X*	X	X	X
Availability	X	X	X	X

Exercise - Steps 4 & 5



4

Select an asset from Step 2:

Health records

Suggestion: select the information asset identified in step 2.

5

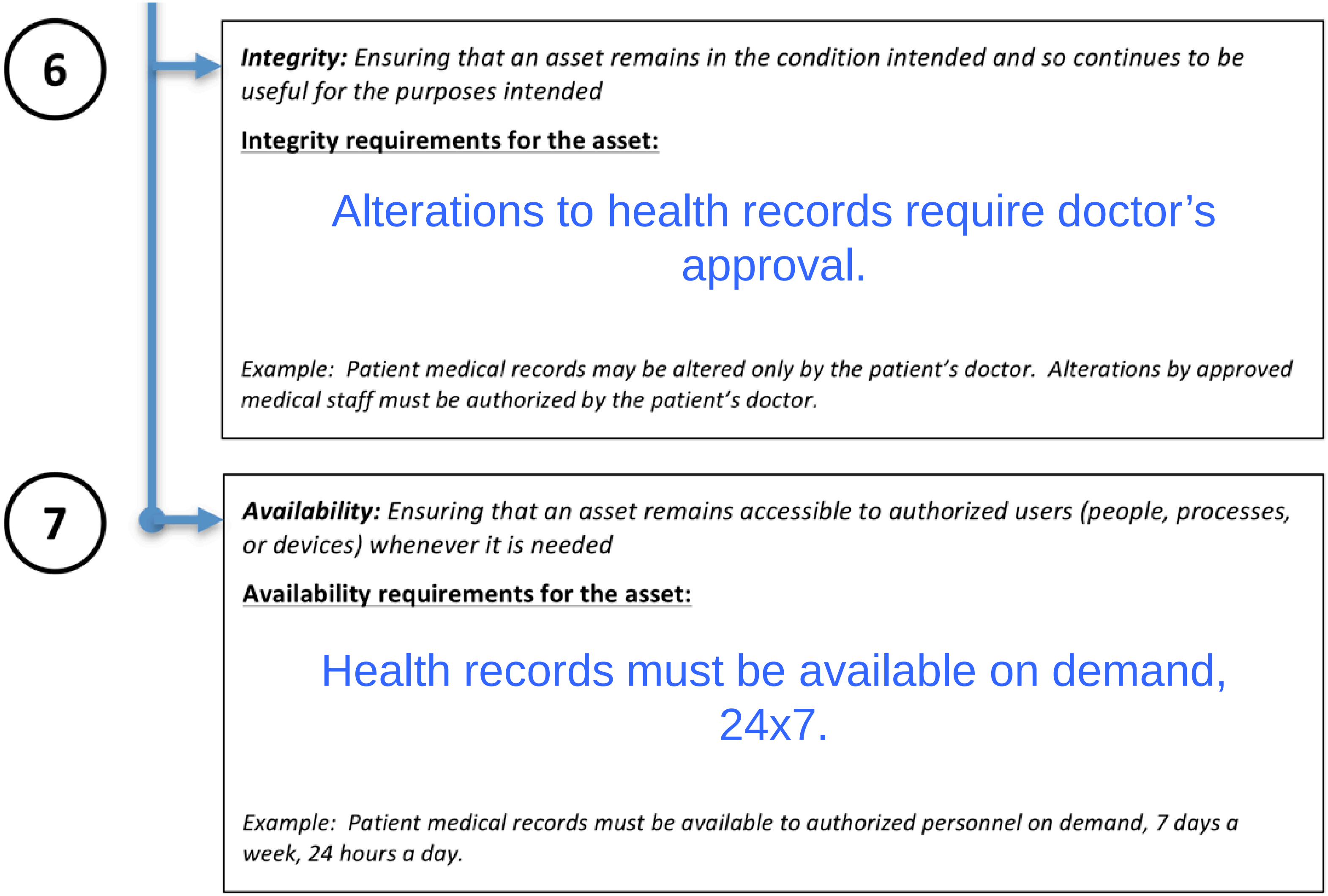
Confidentiality: *Ensuring that only authorized people, processes, or devices have access to an information asset*

Confidentiality requirements for the asset:

Health records may only be accessed by the patient’s doctor and authorized staff.

Example: Patient medical records may only be viewed by the patient’s doctor and medical staff expressly approved by the patient’s doctor.

Exercise - Steps 6 & 7



6

***Integrity:** Ensuring that an asset remains in the condition intended and so continues to be useful for the purposes intended*

Integrity requirements for the asset:

Alterations to health records require doctor's approval.

Example: Patient medical records may be altered only by the patient's doctor. Alterations by approved medical staff must be authorized by the patient's doctor.

7

***Availability:** Ensuring that an asset remains accessible to authorized users (people, processes, or devices) whenever it is needed*

Availability requirements for the asset:

Health records must be available on demand, 24x7.

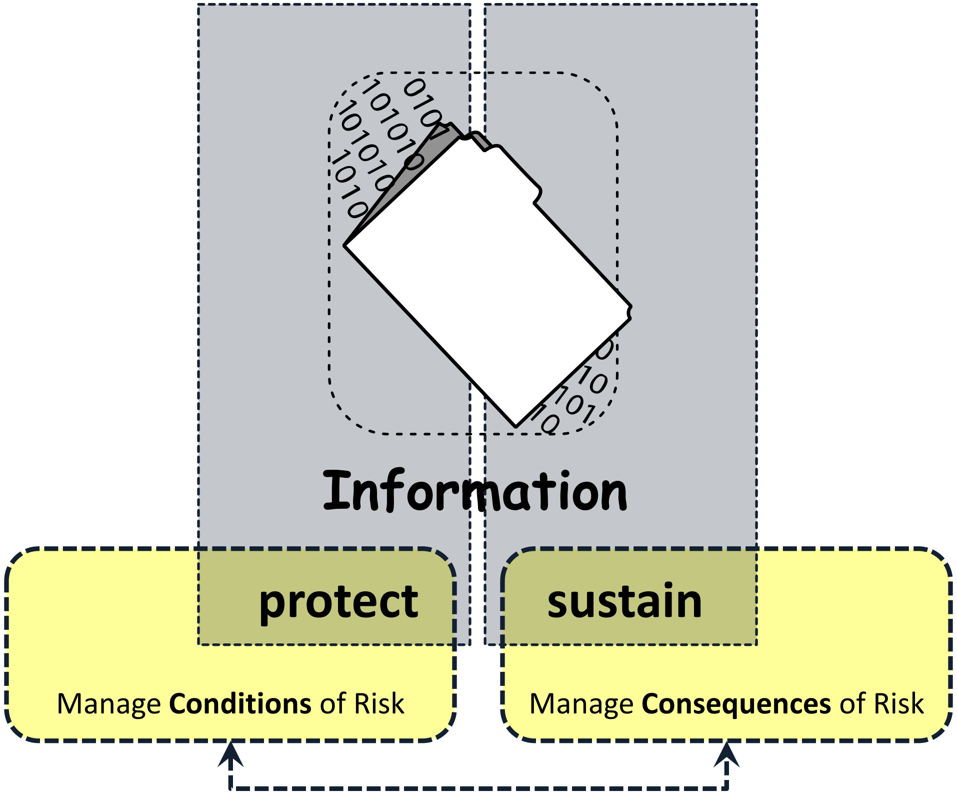
Example: Patient medical records must be available to authorized personnel on demand, 7 days a week, 24 hours a day.

Operational risk and resilience

Operational resilience requires **optimizing** these strategies in a way that

- Minimizes operational risk (to the associated services)
- Makes resource efficient
- Sustains the functionality of the asset.

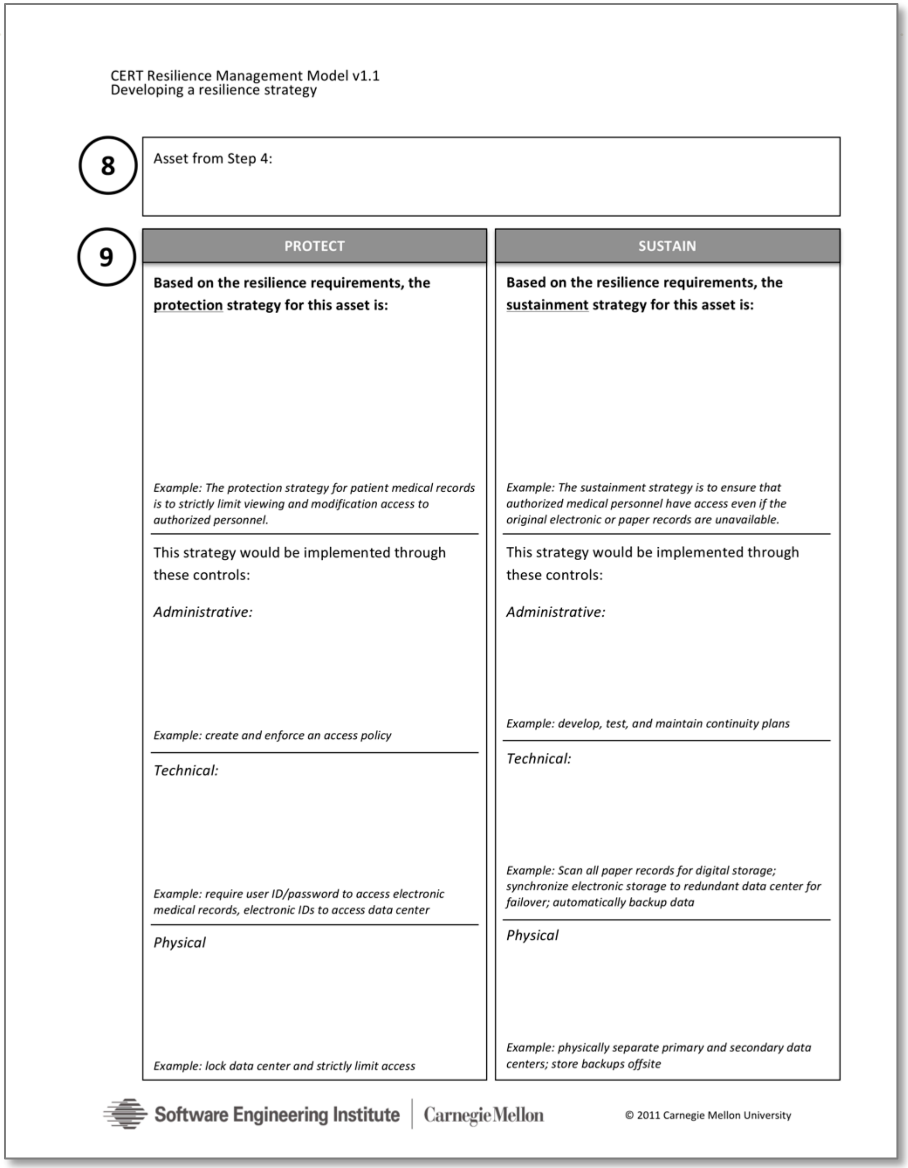
This is the management challenge of operational resilience.



Information
protect
Manage **Conditions** of Risk
sustain
Manage **Consequences** of Risk

Exercise - Steps 8 & 9

Use this part of the exercise worksheet to develop protection and sustainment strategies for your asset



CERT Resilience Management Model v1.1
Developing a resilience strategy

8 Asset from Step 4:

9

PROTECT	SUSTAIN
Based on the resilience requirements, the protection strategy for this asset is:	**Based on the resilience requirements, the sustainment strategy for this asset is:**
Example: The protection strategy for patient medical records is to strictly limit viewing and modification access to authorized personnel.	*Example: The sustainment strategy is to ensure that authorized medical personnel have access even if the original electronic or paper records are unavailable.*
This strategy would be implemented through these controls: *Administrative:*	This strategy would be implemented through these controls: *Administrative:*
Example: create and enforce an access policy	*Example: develop, test, and maintain continuity plans*
Technical:	*Technical:*
Example: require user ID/password to access electronic medical records, electronic IDs to access data center	*Example: Scan all paper records for digital storage; synchronize electronic storage to redundant data center for failover; automatically backup data*
Physical	*Physical*
Example: lock data center and strictly limit access	*Example: physically separate primary and secondary data centers; store backups offsite*

Software Engineering Institute | Carnegie Mellon

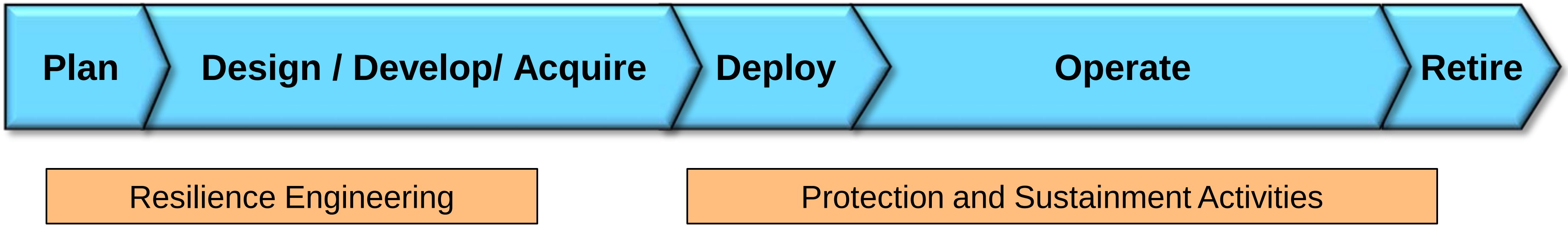
Step-By-Step / Checklist / Roadmap …..

- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment.
- ❑ What are your operational risks? Who will be affected if there are realized?
- ❑ What hurdles do you face to effective operational resilience management?
- ❑ What operational risk management activates (silos) exist? Are there opportunities for convergence of some sort?
- ❑ Draw the resilience context diagram for your organization.
- ❑ What are your resilience requirement categories?
- ❑ Repeat the exercise for your organization.

Cornerstones of Operational Resilience

- ✓ Risk Management
  - Operational Risk Management
- ✓ Convergence
- ✓ Organizational Construct for Resilience Activities
- ✓ Protection and Sustainment Activities
- Lifecycle View
- Institutionalization

Lifecycle View


Plan
Design / Develop/ Acquire
Deploy
Operate
Retire
Resilience Engineering
Protection and Sustainment Activities

To improve and sustain an entity's operational resilience, it is not sufficient to only improve protection and sustainment activities.

resilience should not be an afterthought bolt-on

resilience should be engineered and built-in

Resilience Management is a Total Lifecycle Concept

Cornerstones of Operational Resilience

- ✓ Risk Management
  - Operational Risk Management
- ✓ Convergence
- ✓ Organizational Construct for Resilience Activities
- ✓ Protection and Sustainment Activities
- ✓ Lifecycle View
- Institutionalization

What do these organizations have in common?

Customer Happiness

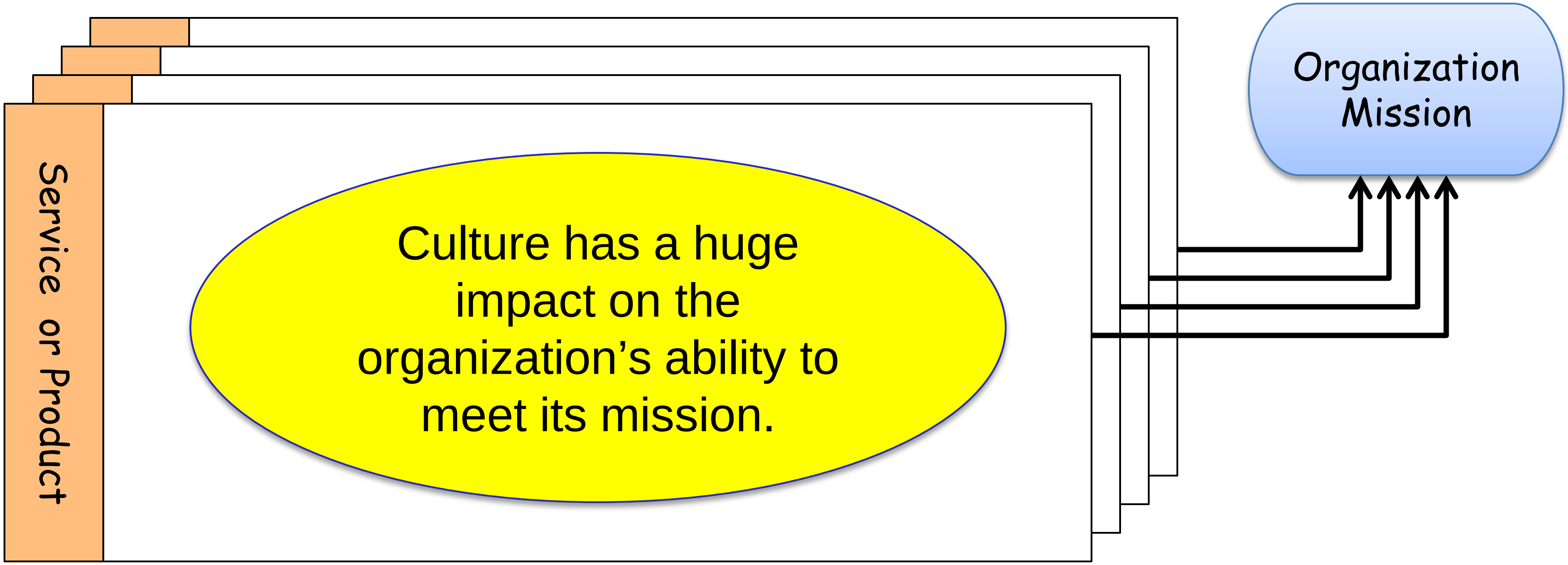
Chain of Command
Unit Cohesion
Regulations

Strong Culture

Customer Service

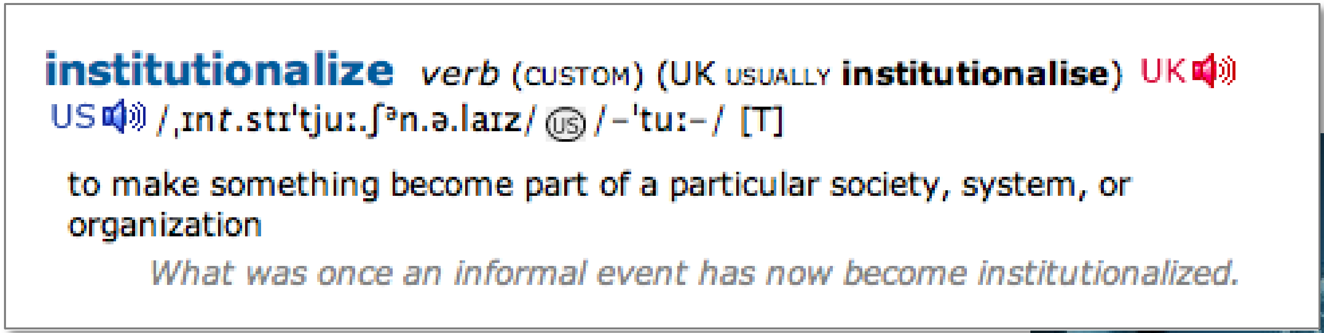
Tradition
Protection

Institutionalizing a Culture of resilience



Culture has a huge impact on the organization's ability to meet its mission.

Institutionalizing a Culture of resilience



institutionalize *verb* (CUSTOM) (UK USUALLY **institutionalise**) UK 🔊
US 🔊 /ˌɪnt.stɪˈtjuː.ʃᵊn.ə.laɪz/ (US) /-ˈtuː-/ [T]

to make something become part of a particular society, system, or organization

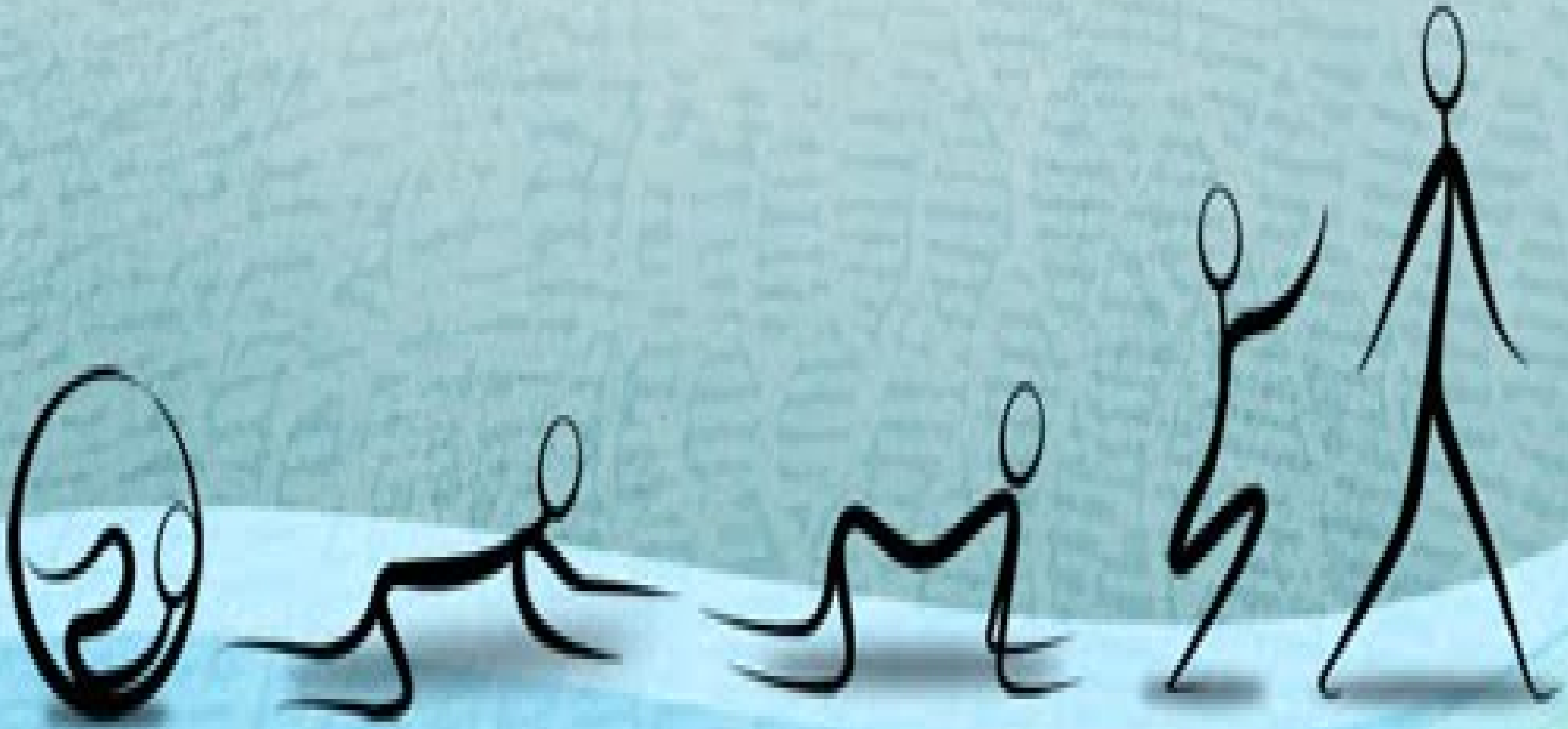
What was once an informal event has now become institutionalized.

Organizations must provide explicit guidance for institutionalizing resilience activities so that they persist over time

Ask not how well am I performing today?

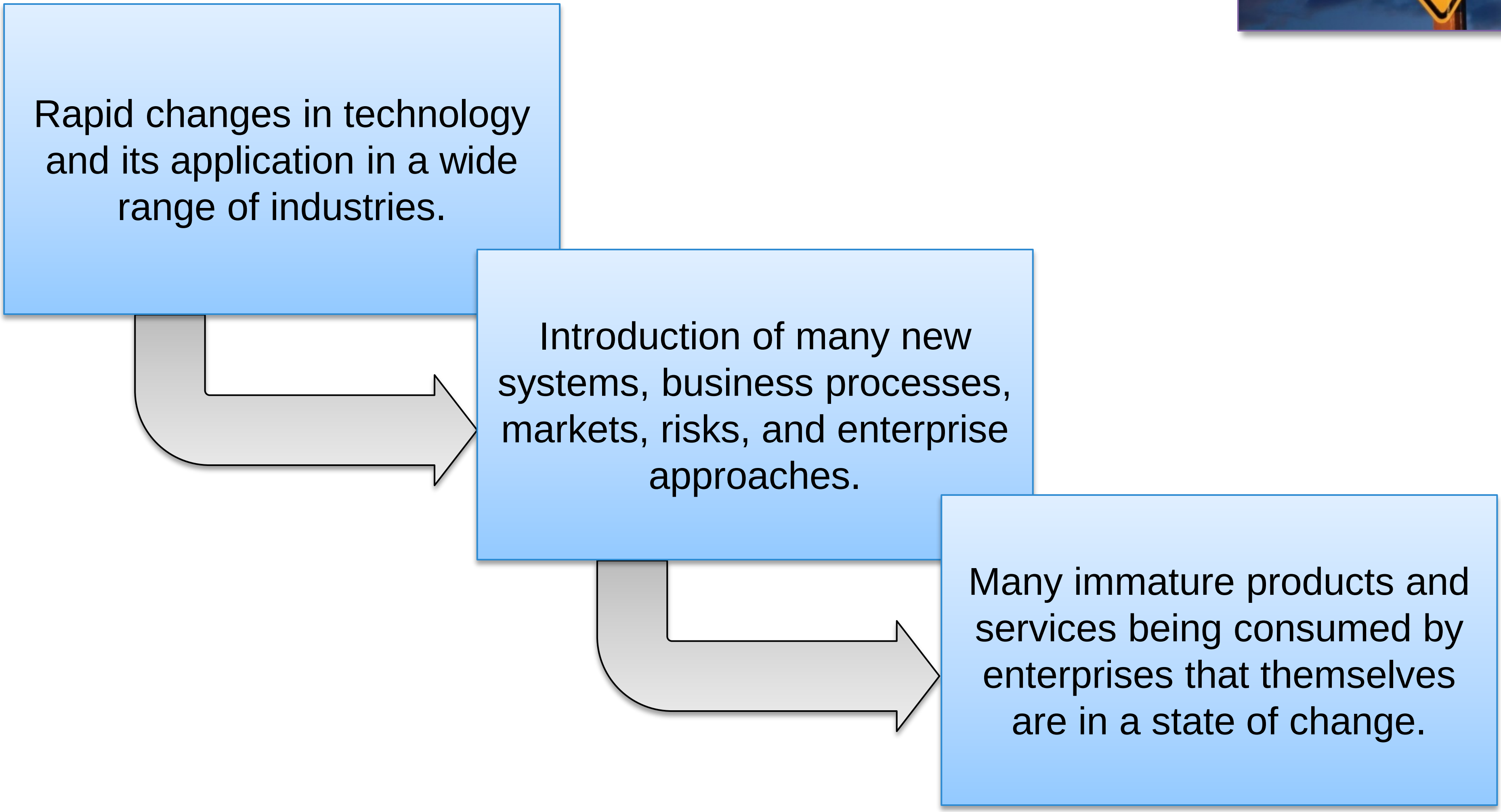
Ask do I have what it takes to sustain high performance beyond today?

Is there one place that I can go to see what are all the right things that an organization should do in order to improve and manage its operational resilience in a systematic, practical, and proven manner?



Maturity Models

Today’s Operating Environment



Rapid changes in technology and its application in a wide range of industries.

Introduction of many new systems, business processes, markets, risks, and enterprise approaches.

Many immature products and services being consumed by enterprises that themselves are in a state of change.

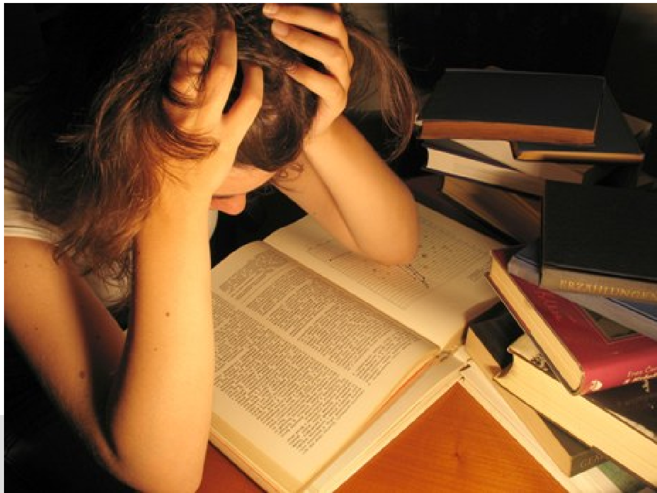
Challenges at Hand

How can you tell if you are doing a good job of managing these changes?

What are effective ways to monitor your progress?

How do you manage the interactions of systems and processes that are continually changing?

How do poor processes impact interoperability, safety, reliability, efficiency, and effectiveness?

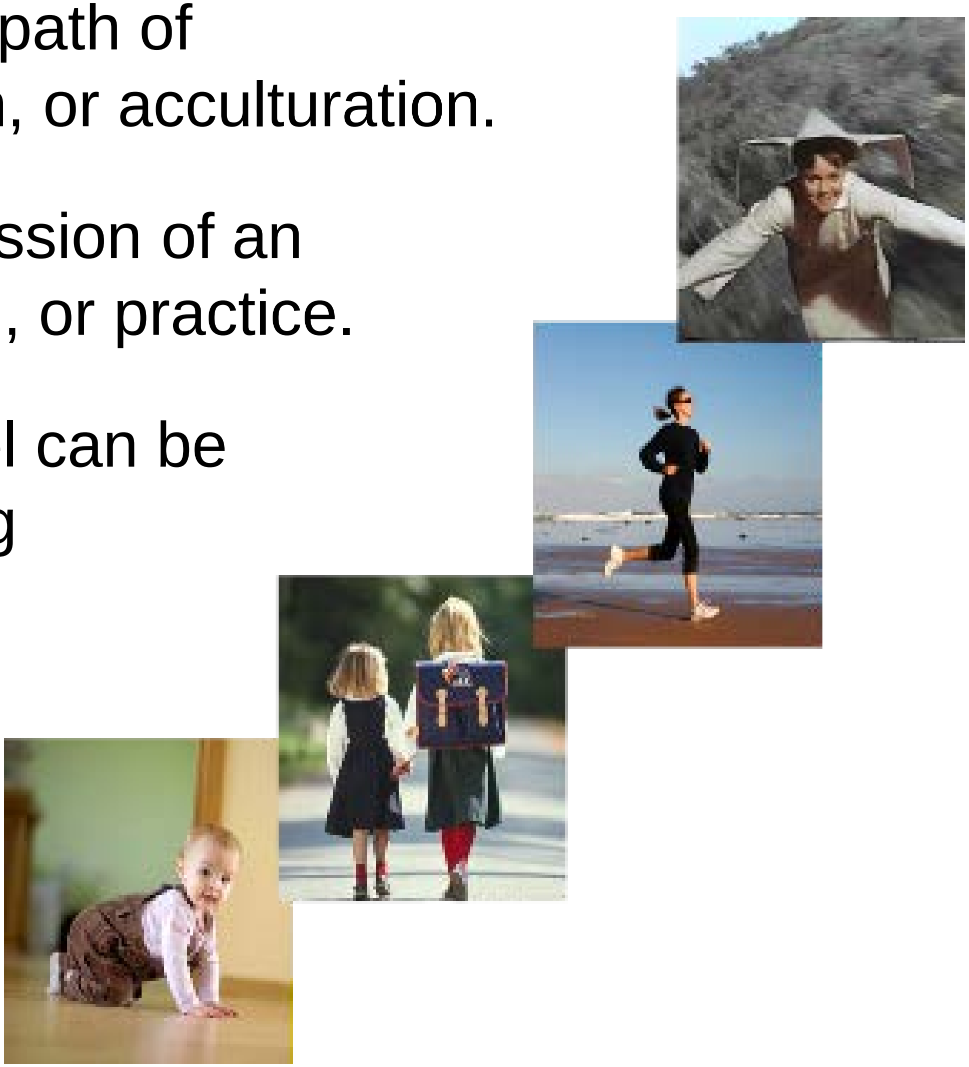


Maturity Model Defined

An organized way to convey a path of experience, wisdom, perfection, or acculturation.

Depicts an evolutionary progression of an attribute, characteristic, pattern, or practice.

The subject of a maturity model can be objects or things, ways of doing something, characteristics of something, practices, controls, or processes.



Maturity Models Provide…

Means for assessing and benchmarking performance

Ability to assess how a set of characteristics have evolved

Expression of a body of knowledge of best practices

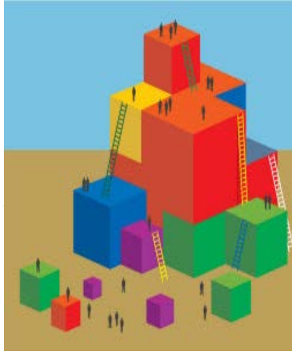
Means to identify gaps and develop improvement plans

Roadmap for model-based improvement

Demonstrated results of improvement efforts

Common language or taxonomy

Key Components of a Maturity Model



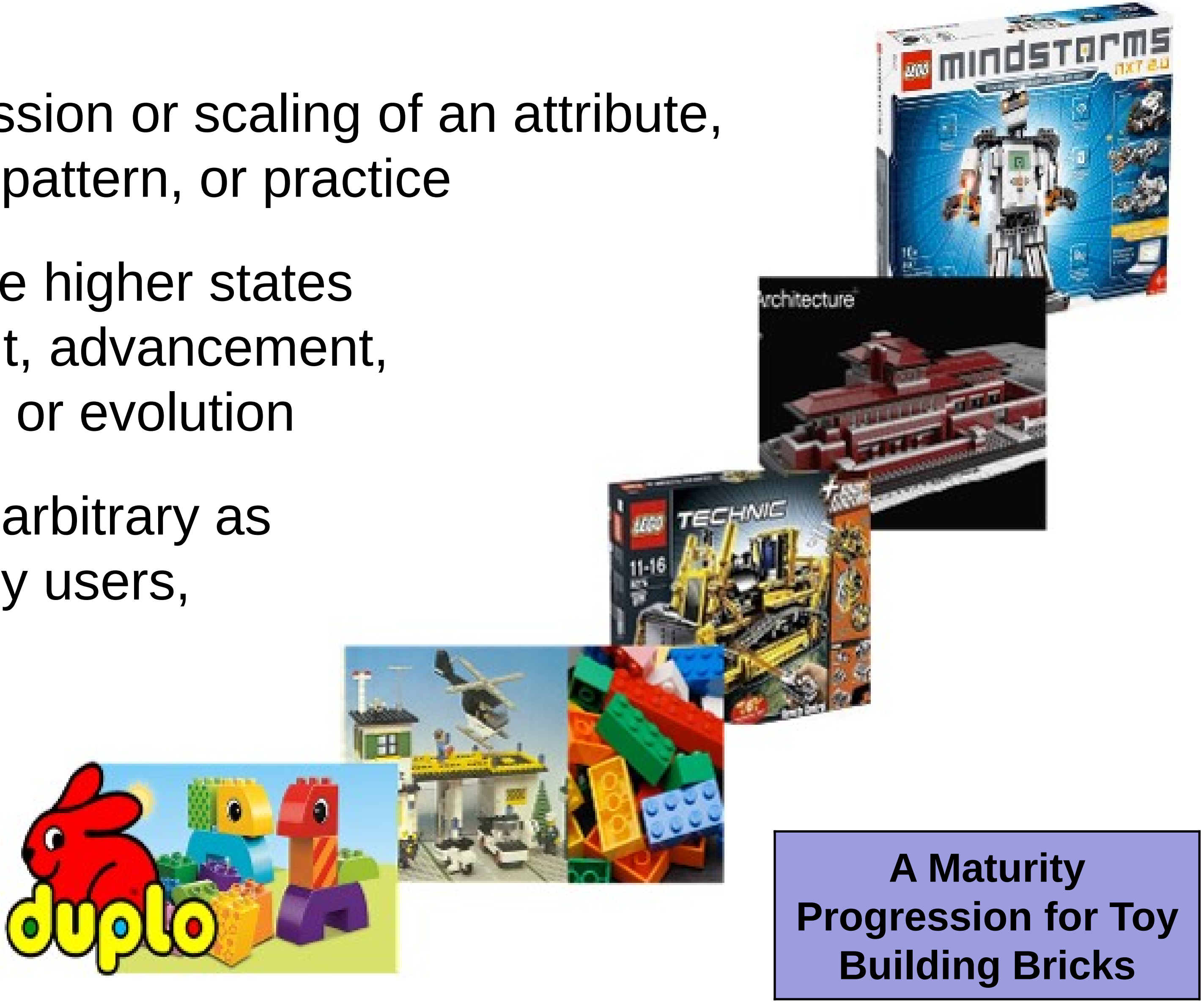
Levels	• The measurement scale • The transitional states
Domains	• Logical groupings of like attributes into areas of importance to the subject matter and intent of the model • Logical groupings of like practices, processes, or good things to do
Attributes	• Core content of the model arranged by domains and levels • Typically based on observed practices, standards, or expert knowledge
Diagnostic Methods	• For assessment, measurement, gap identification, benchmarking
Improvement Roadmaps	• To guide improvement efforts (Plan-Do-Check-Act; Observe-Orient-Decide-Act)

Progression Model Defined

Simple progression or scaling of an attribute, characteristic, pattern, or practice

Levels describe higher states of achievement, advancement, completeness, or evolution

Levels can be arbitrary as agreed upon by users, industry, etc.



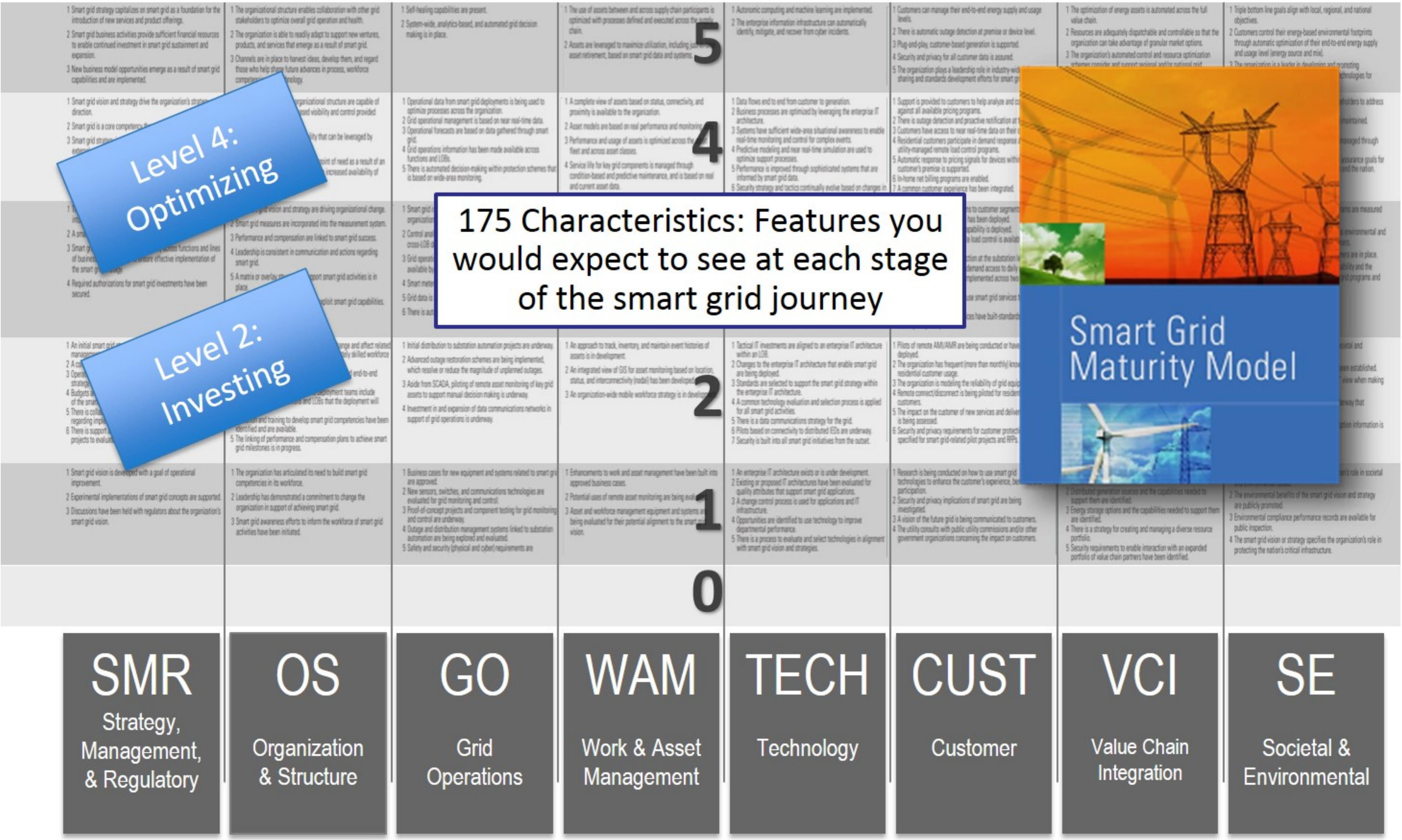
A Maturity Progression for Toy Building Bricks

Progression Model Example

A Maturity Progression for Authentication
Three-factor authentication
Two-factor authentication
Addition of changing every 60 days
Use of strong passwords
Use of simple passwords`

A Maturity Progression for Human Mobility
Fly
Sprint
Run
Jog
Walk
Crawl

Progression Model Example: SGMM



175 Characteristics: Features you would expect to see at each stage of the smart grid journey

Benefits & Limitations of Progression Models

Benefits

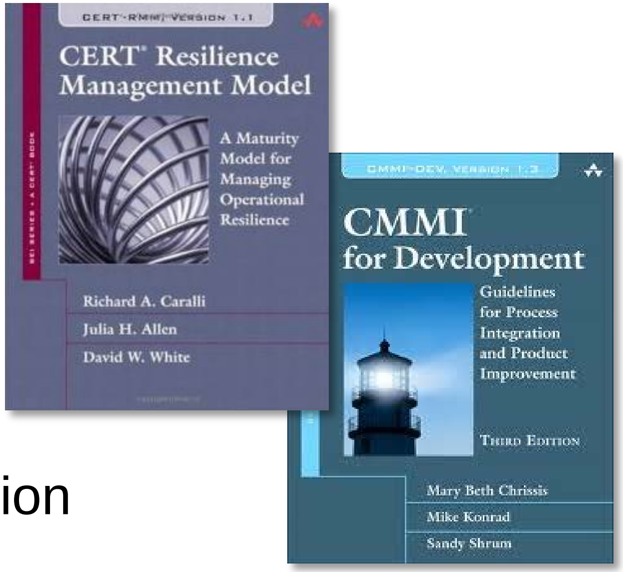
- Provides a transformative roadmap
- Simple to understand and adopt; low adoption cost
- Easy to recalibrate as technologies and practices advance

Limitations

- Levels are arbitrarily defined and may be meaningless for achieving objectives
- Achieving higher levels does not necessarily translate into “maturity”
- Often confused with CMMs - thus users inaccurately project traits of CMMs on progression models

Capability Maturity Models (CMM)

- A more complex instrument
- Characterizes
  - the maturity of processes
  - the degree to which processes are institutionalized
  - the maturity of the culture of the organization
  - the extent to which the organization demonstrates process maturity
- Levels reflect the extent to which a particular set of practices have been institutionalized
  - Institutionalized processes are more likely to be retained during times of stress.

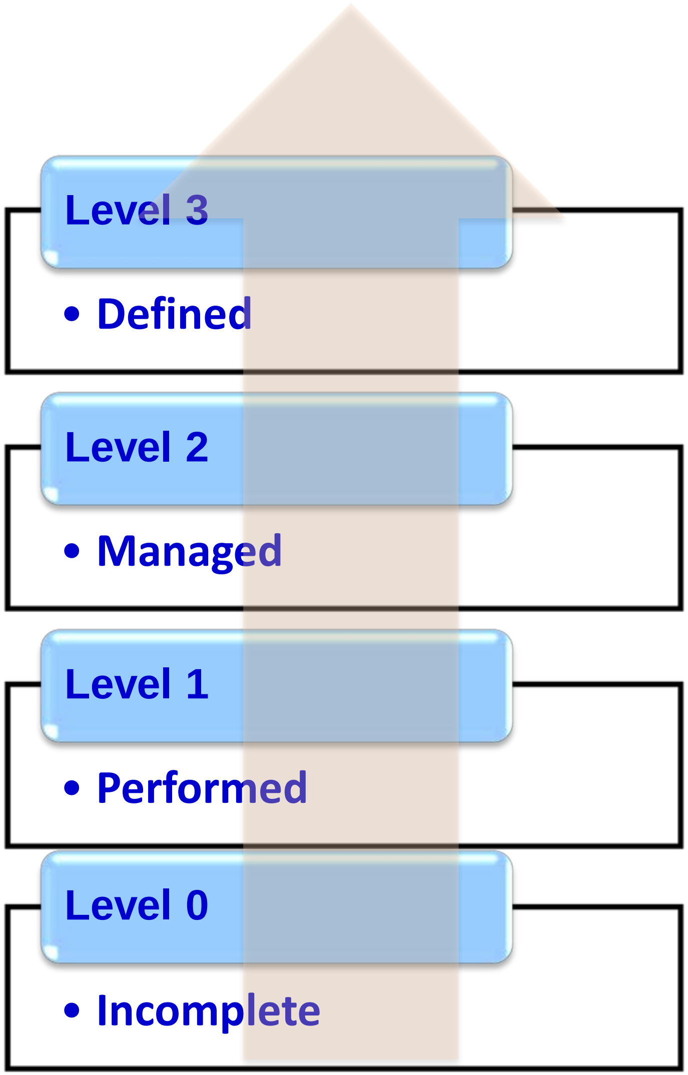


Capability Maturity Model Levels

Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete



Level 3
- Defined

Level 2
- Managed

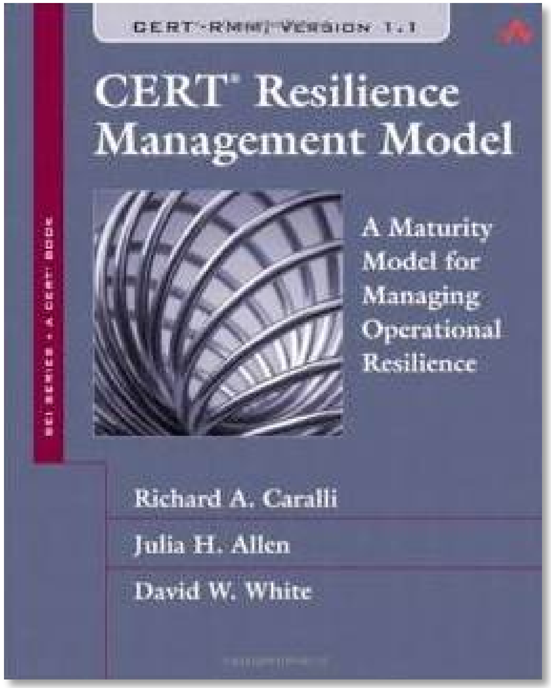
Level 1
- Performed

Level 0
- Incomplete

Higher degrees of institutionalization translate to more stable processes that

- *are repeatable*
- *produce consistent results over time*
- *are retained during times of stress*

Capability Maturity Model Example: CERT-RMM


CERT®-RMM| VERSION 1.1
CERT® Resilience Management Model
A Maturity Model for Managing Operational Resilience
Richard A. Caralli
Julia H. Allen
David W. White
SEI SERIES • A CERT® BOOK

Framework for managing and improving operational resilience

"…an extensive super-set of the things an organization could do to be more resilient."

- CERT-RMM adopter

http://www.cert.org/resilience/

Benefits and Limitations of CMMs

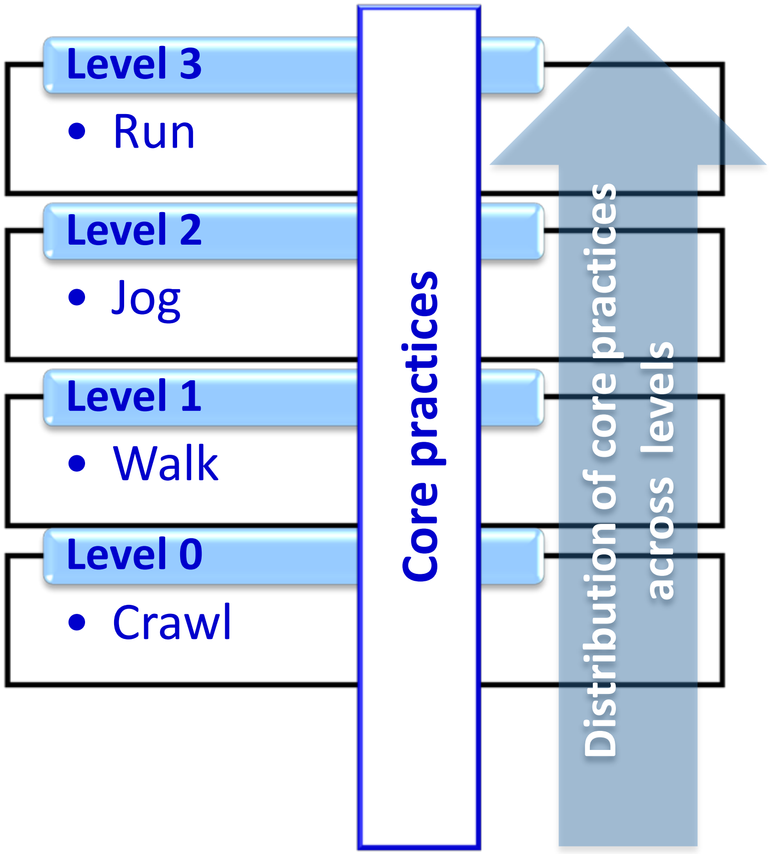
Benefits

- Provides for measurement of core competencies
- Provides for rigorous measurement of capability—the ability to retain core competencies under times of stress
- Can provide a path to quantitative measurement

Limitations

- Sometimes difficult to understand and apply; high adoption cost
- “Maturity” may not translate into actual results
- Potential false sense of achievement: achieving high maturity in security practices may not mean the organization is “secure”

Compare: Progression vs CMM



Level 3

- Run

Level 2

- Jog

Level 1

- Walk

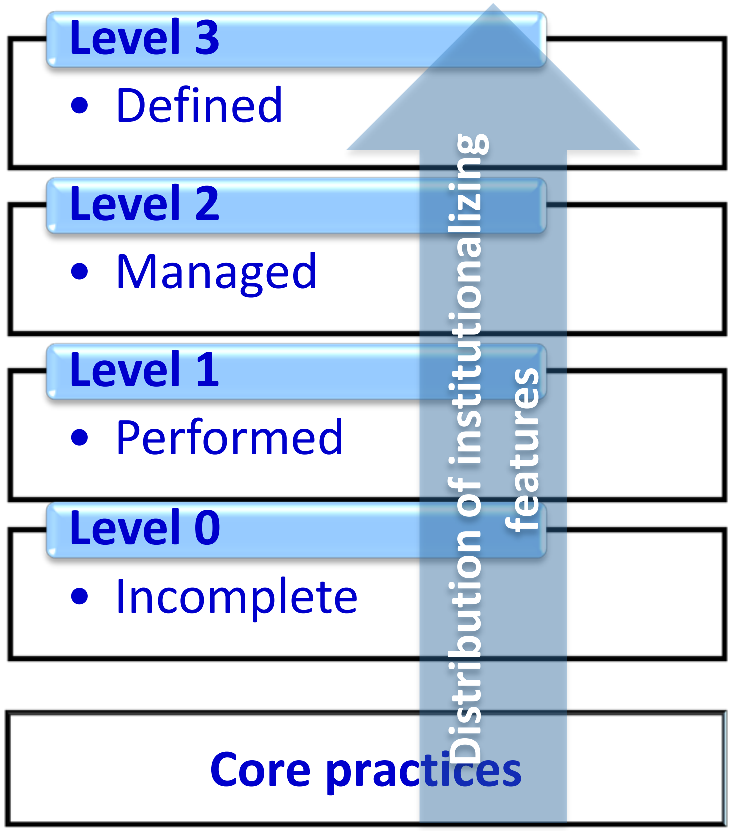
Level 0

- Crawl

Core practices

Distribution of core practices across levels

Progression Model



Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

Level 0

- Incomplete

Core practices

Distribution of institutionalizing features

Capability Model

Hybrid Models

Combine best features of progression and capability maturity models

- Allow for measurement of evolution or achievement as in progression models
- Add the ability to measure capability or institutionalization with the rigor of a CMM

Levels reflect both achievement and capability

Transitions between levels:

- Similar to a capability model (i.e., describe capability maturity)
- Architecturally use the characteristics, indicators, attributes, or patterns of a progression model

Hybrid Model

Domains: Specific categories of attributes, characteristics, patterns, or practices that form the content of the model

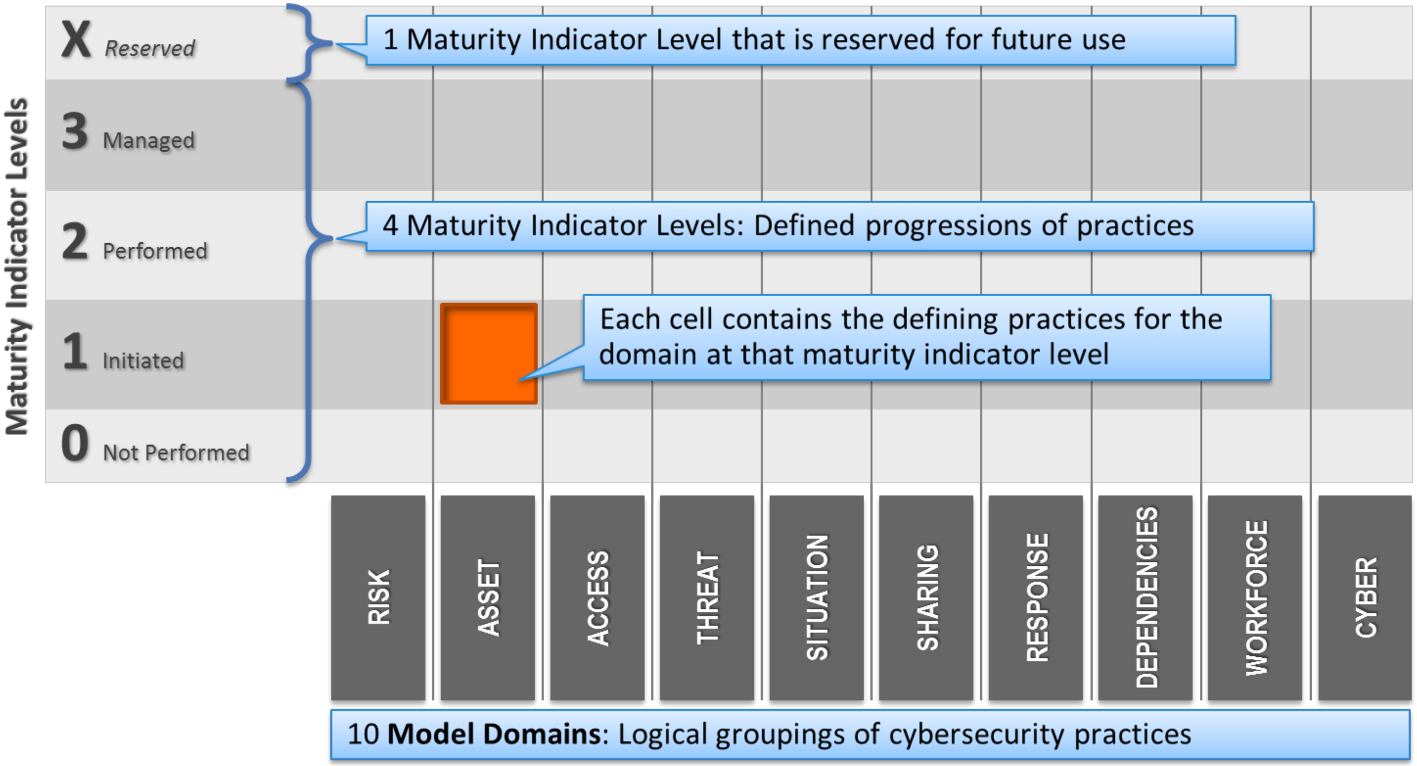
Capability or “maturity” levels

	Domain 1	Domain 2	Domain 3	Domain 4	Domain *n*
Level 4 *Defined*					
Level 3 *Measured*					
Level 2 *Managed*					
Level 1 *Planned*					
Level 0 *Incomplete*					

Model content: Specific attributes, characteristics, patterns, or practices that represent **progression** and **capability**

Maturity Levels: Defined sets of characteristics and outcomes, ***plus capability considerations***

Hybrid Model Example: ES-C2M2



Maturity Indicator Levels

X *Reserved*

3 Managed

2 Performed

1 Initiated

0 Not Performed

1 Maturity Indicator Level that is reserved for future use

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level

RISK

ASSET

ACCESS

THREAT

SITUATION

SHARING

RESPONSE

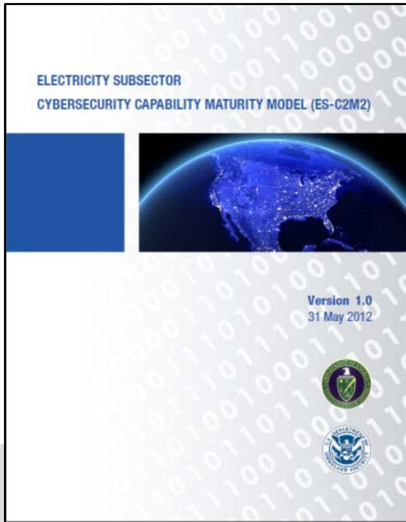
DEPENDENCIES

WORKFORCE

CYBER

10 **Model Domains**: Logical groupings of cybersecurity practices

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0
31 May 2012

When Does It Make Sense to Use Maturity Models?

Requirement for a structured approach

Demonstrated, measurable results based on an established body of knowledge

A defined roadmap from a current state to a desired state

An ability to monitor and measure progress, particularly in the presence of change

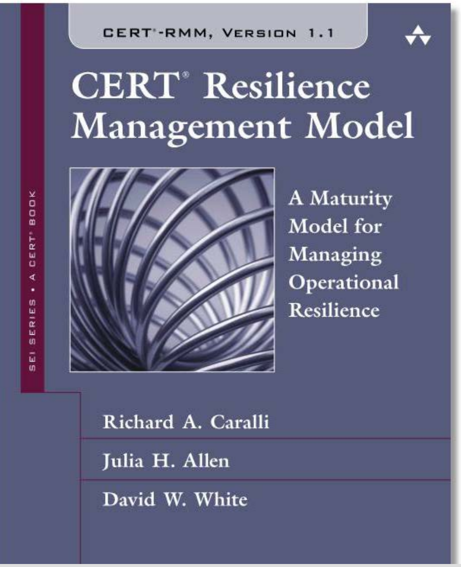
- Response to a strategic improvement or new product/new market objective

When Does It Make Sense to Use Maturity Models? *(cont.)*

Desire to answer these questions in a repeatable, predictable manner:

- How do I compare with my peers? (ability to benchmark)
- How can I determine how secure I am and if I am secure enough?
- How do I measure my current state? Characterize my desired state?
- What concrete actions do I need to take to improve? And in what order?
- How do I measure progress toward my desired state?
- How do I adapt to change?

Overview of CERT Resilience Management Model (CERT-RMM)



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI Series • A CERT® Book

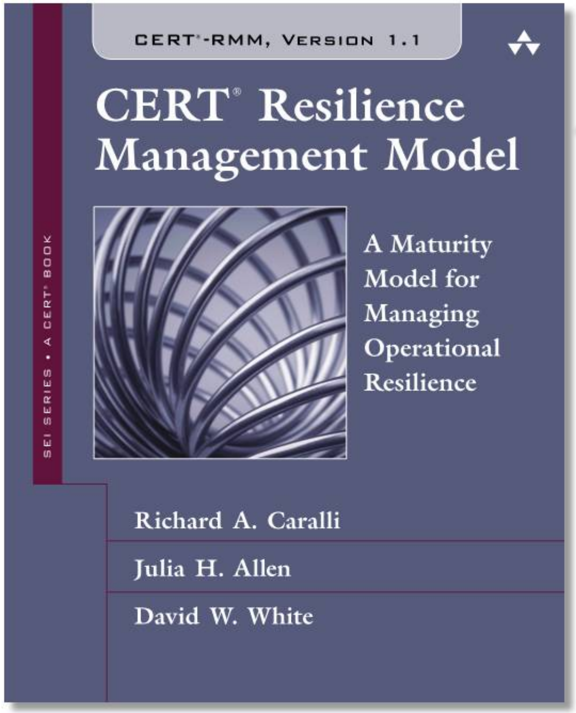
Richard A. Caralli

Julia H. Allen

David W. White

Background & History

CERT Resilience Management Model (CERT-RMM)


CERT®-RMM, Version 1.1
CERT® Resilience Management Model
A Maturity Model for Managing Operational Resilience
SEI Series • A CERT® Book
Richard A. Caralli
Julia H. Allen
David W. White

Framework for managing and improving operational resilience

http://www.cert.org/resilience/

"…an extensive super-set of the things an organization could do to be more resilient."

- CERT-RMM adopter

What is CERT-RMM?

Guides implementation and management of operational resilience activities

Enables and promotes the **convergence** of

- COOP, IT Disaster Recovery, Business Continuity
- Information Security, Cyber security
- IT Operations

A capability model for managing & improving operational resilience

- Defines maturity through capability levels
- Enables assessment and measurement

What is CERT-RMM? (Cont.)

Applicable to a variety of organizations

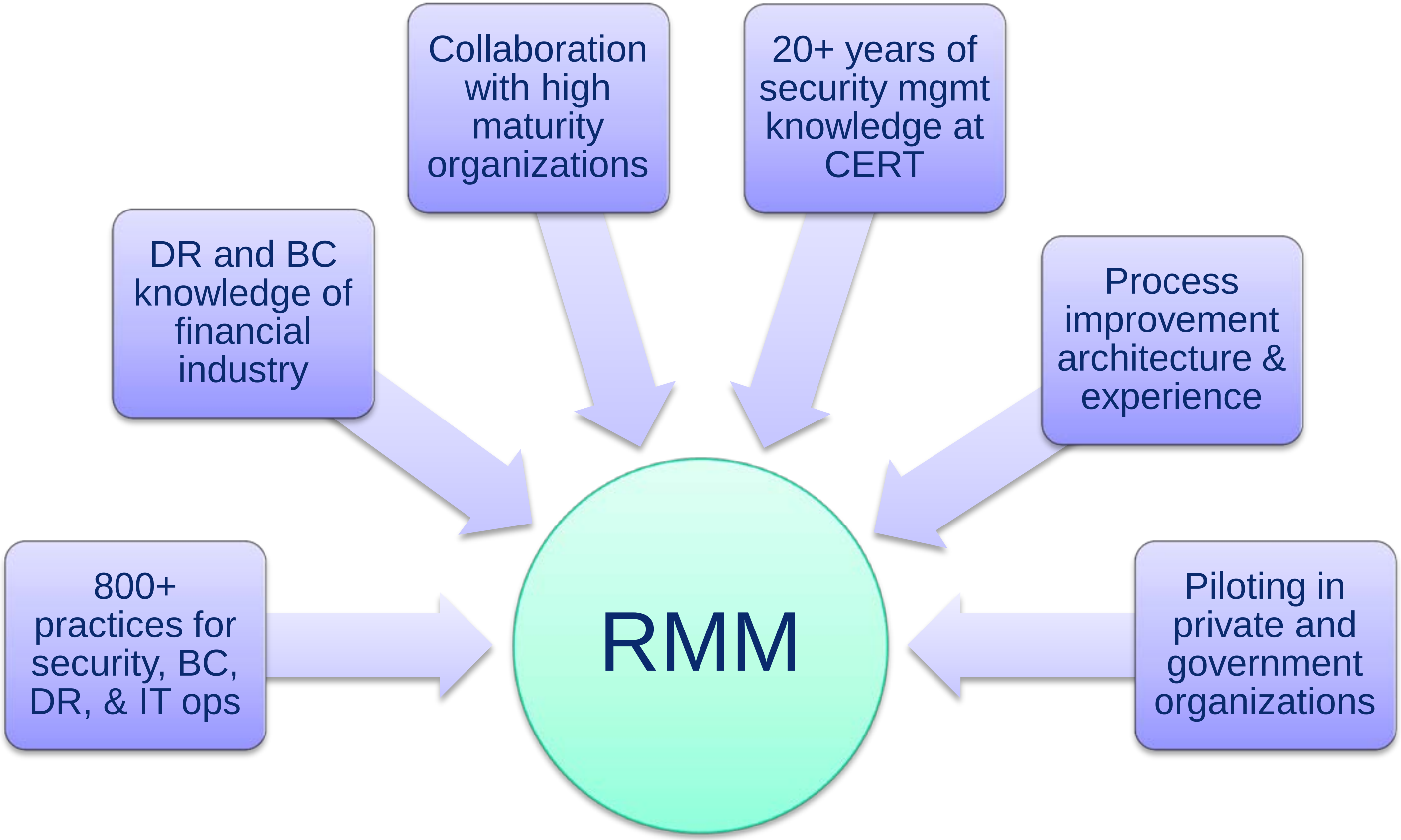
- small or large
- simple or complex
- public or private

Descriptive rather than prescriptive

- Focuses on the “what” not the “how”

Improves confidence in how an organization responds in times of operational stress

How was RMM developed?



Collaboration with high maturity organizations

20+ years of security mgmt knowledge at CERT

DR and BC knowledge of financial industry

Process improvement architecture & experience

800+ practices for security, BC, DR, & IT ops

RMM

Piloting in private and government organizations

RMM codifies best practices for Info. Sec., IT DR, and BC from world leading organizations and numerous standards and codes of practice.

What drove development of RMM?

Increasingly complex operational environments

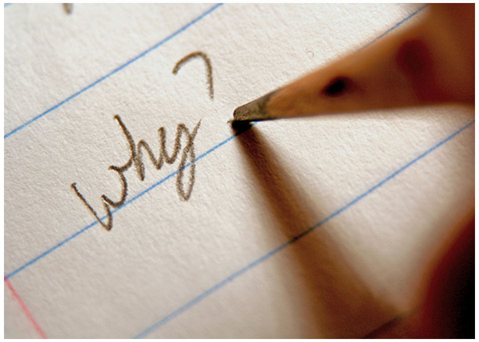
Siloed nature of operational risk activities

Lack of common language or taxonomy

Overreliance on technical approaches

Lack of means to measure organizational capability

Inability to confidently predict outcomes, behaviors, and performance under times of stress



RMM – The Model

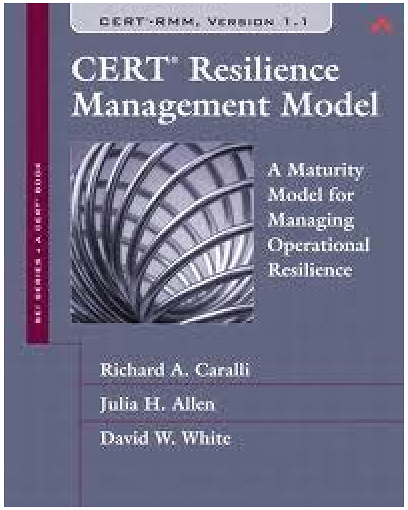
Guidelines and practices for

- Converging of security, business continuity, disaster recovery, and IT ops
- Implementing, managing, and sustaining operational resilience activities
- Managing operational risk through process
- Measuring and institutionalizing the Resilience process

Common vernacular and basis for planning, communicating, and evaluating improvements

Focuses on “what” not “how”

Organized into 26 process areas

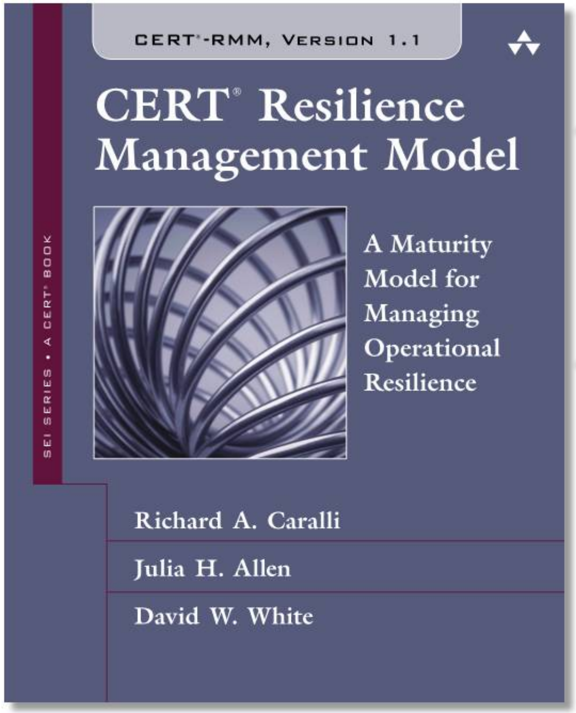

CERT-RMM, Version 1.1
CERT® Resilience Management Model
A Maturity Model for Managing Operational Resilience
Richard A. Caralli
Julia H. Allen
David W. White

RMM Process Areas

- Access Management
- Asset Definition and Management
- Communications
- Compliance
- Controls Management
- Enterprise Focus
- Environmental Control
- External Dependencies
- Financial Resource Management
- Human Resource Management
- Identity Management
- Incident Management & Control
- Knowledge & Information Mgmt

- Measurement and Analysis
- Monitoring
- Organizational Process Focus
- Organizational Process Definition
- Organizational Training & Awareness
- People Management
- Resilience Requirements Development
- Resilience Requirements Management
- Resilient Technical Solution Engr.
- Risk Management
- Service Continuity
- Technology Management
- Vulnerability Analysis & Resolution

CERT Resilience Management Model (CERT-RMM)



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI Series • A CERT® Book

Richard A. Caralli

Julia H. Allen

David W. White

http://www.cert.org/resilience/

Framework for managing and improving operational resilience

A process improvement model

"…an extensive super-set of the things an organization could do to be more resilient."

—CERT-RMM adopter

Core Principle and Focus of RMM

System or Product Perspective

The quality of a system or product is highly influenced by the quality of the process used to acquire, develop, and maintain it.

→

Transforming the quality of the product (output) by transforming the process by which the product is developed and produced.

Operational Resilience Perspective

The ability of the organization to sustain operations in the face of operational risk is highly influenced by the quality of the process used to ensure assets remain protected and sustained.

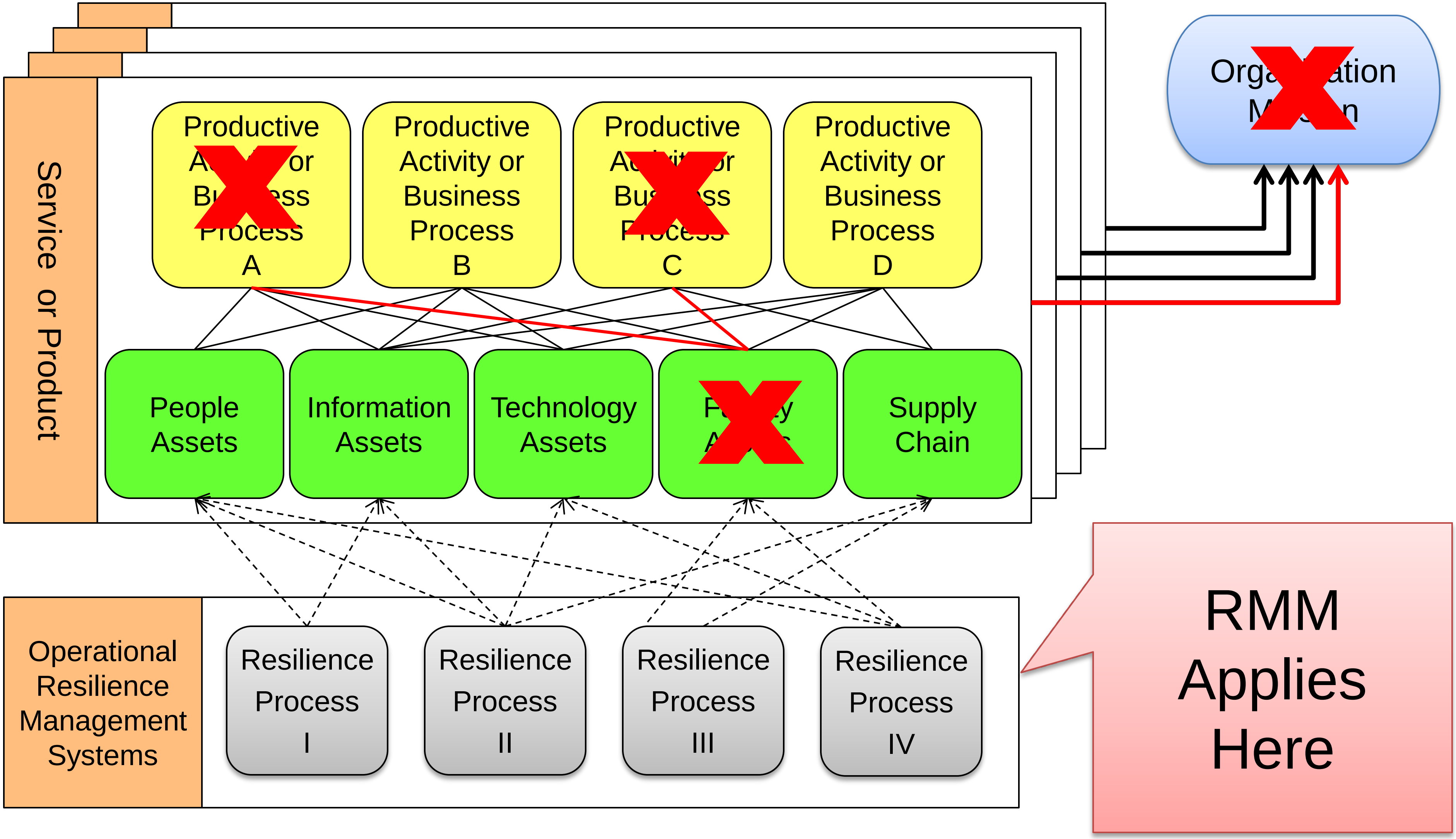
→

Transforming some (emergent) quality of the organization, called operational resilience, by focusing on the processes of activities that support operational resilience management systems.

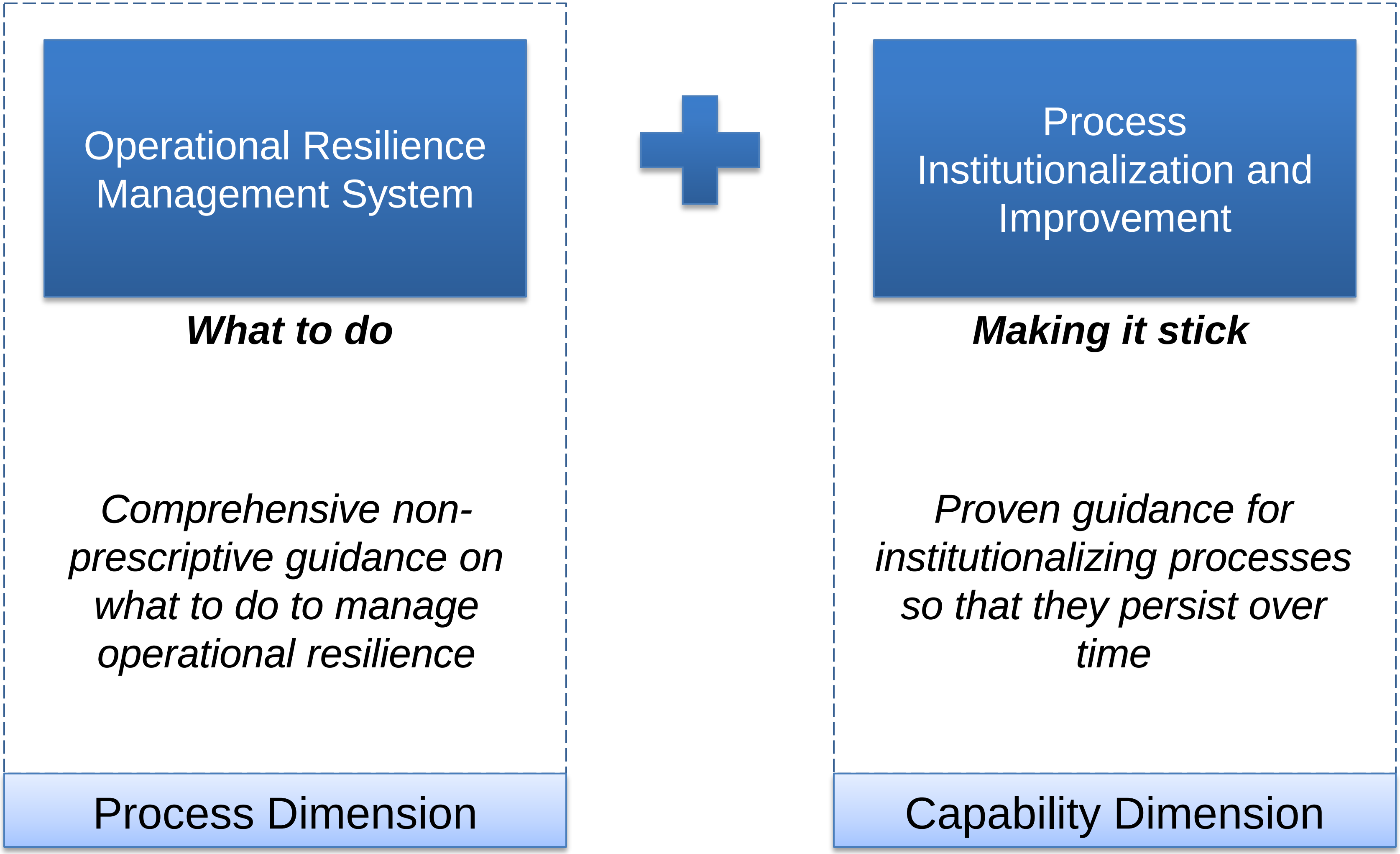
Foundational Elements of CERT-RMM

- Operational Resilience
    - Operational Risk Management
- Convergence
- Organizational Construct for Resilience Activities
- Protection & Sustainment Activities
- Institutionalization
- Institutionalization
    - Capability Dimension
- Lifecycle View
- Code of Practice Crosswalk

Organizational Context for Resilience Activities



RMM Combines Two Approaches



Operational Resilience Management System

What to do

Comprehensive non-prescriptive guidance on what to do to manage operational resilience

Process Dimension

Process Institutionalization and Improvement

Making it stick

Proven guidance for institutionalizing processes so that they persist over time

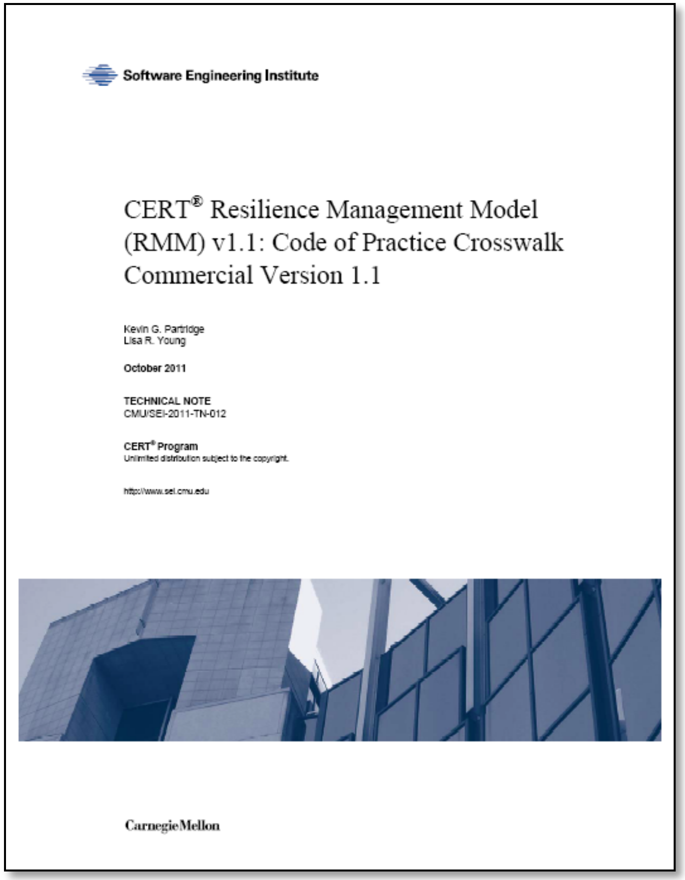
Capability Dimension

Code of Practice Crosswalk

Links RMM practices to common used codes of practice and standards

Including:

- ANSI/ASIS SPC.1-2009
- BS25999
- COBIT 4.1
- COSO ERM Framework
- CMMI
- FFIEC BCP Handbook
- ISO 20000-2
- ISO/IEC 24762
- ISO/IEC 24762
- ISO/IEC 27005
- ISO/IEC 31000
- NFPA 1600
- PCI DSS
- Etc…



Software Engineering Institute

CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1

Kevin G. Partridge
Lisa R. Young

October 2011

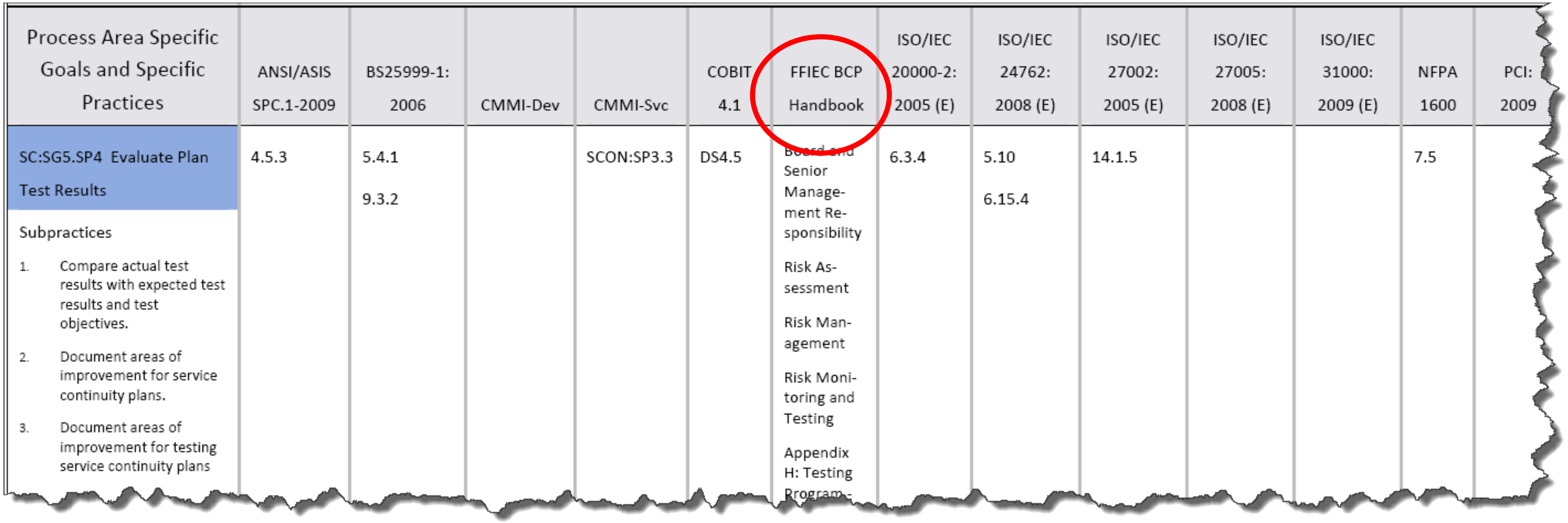
TECHNICAL NOTE
CMU/SEI-2011-TN-012

CERT® Program
Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

CarnegieMellon

RMM Code of Practice Crosswalk

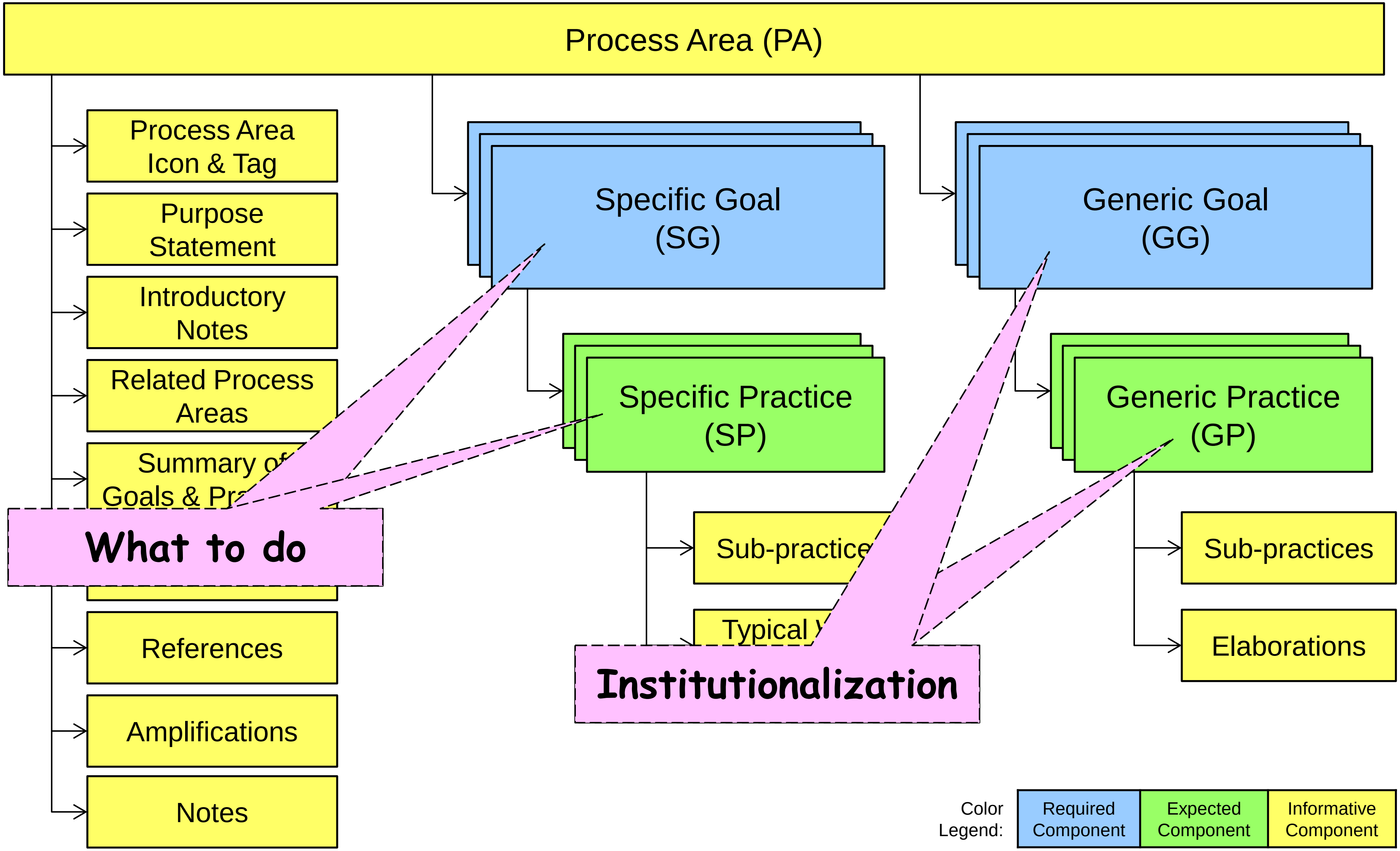


Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG5.SP4 Evaluate Plan Test Results	4.5.3	5.4.1 9.3.2		SCON:SP3.3	DS4.5	Board and Senior Management Responsibility Risk Assessment Risk Management Risk Monitoring and Testing Appendix H: Testing Program -	6.3.4	5.10 6.15.4	14.1.5			7.5	
Subpractices 1. Compare actual test results with expected test results and test objectives. 2. Document areas of improvement for service continuity plans. 3. Document areas of improvement for testing service continuity plans													

Extensive Tabular Crosswalk between RMM's 26 Process Areas and 251 Specific Practices and Key Industry Standards

Organization of the Model

Process Area Structure & Components



Process Area (PA)

Process Area Icon & Tag

Purpose Statement

Introductory Notes

Related Process Areas

Summary of Goals & Pr

References

Amplifications

Notes

Specific Goal (SG)

Specific Practice (SP)

Sub-practice

Typical W

Generic Goal (GG)

Generic Practice (GP)

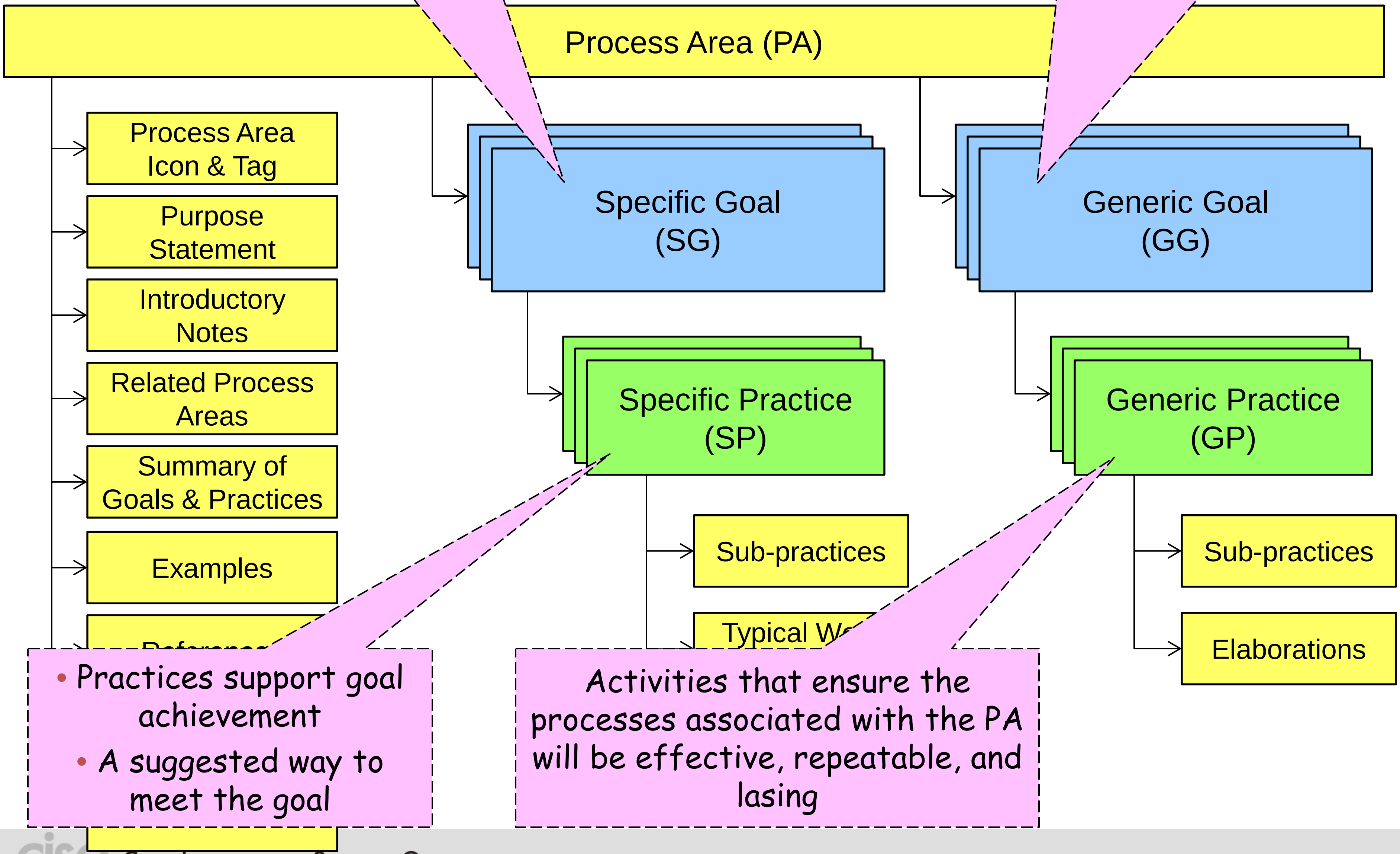
Sub-practices

Elaborations

What to do

Institutionalization

Color Legend:	Required Component	Expected Component	Informative Component



Describes "what" to do to achieve the capability

Describes the characteristics that must be present to institutionalize the processes that implement a PA

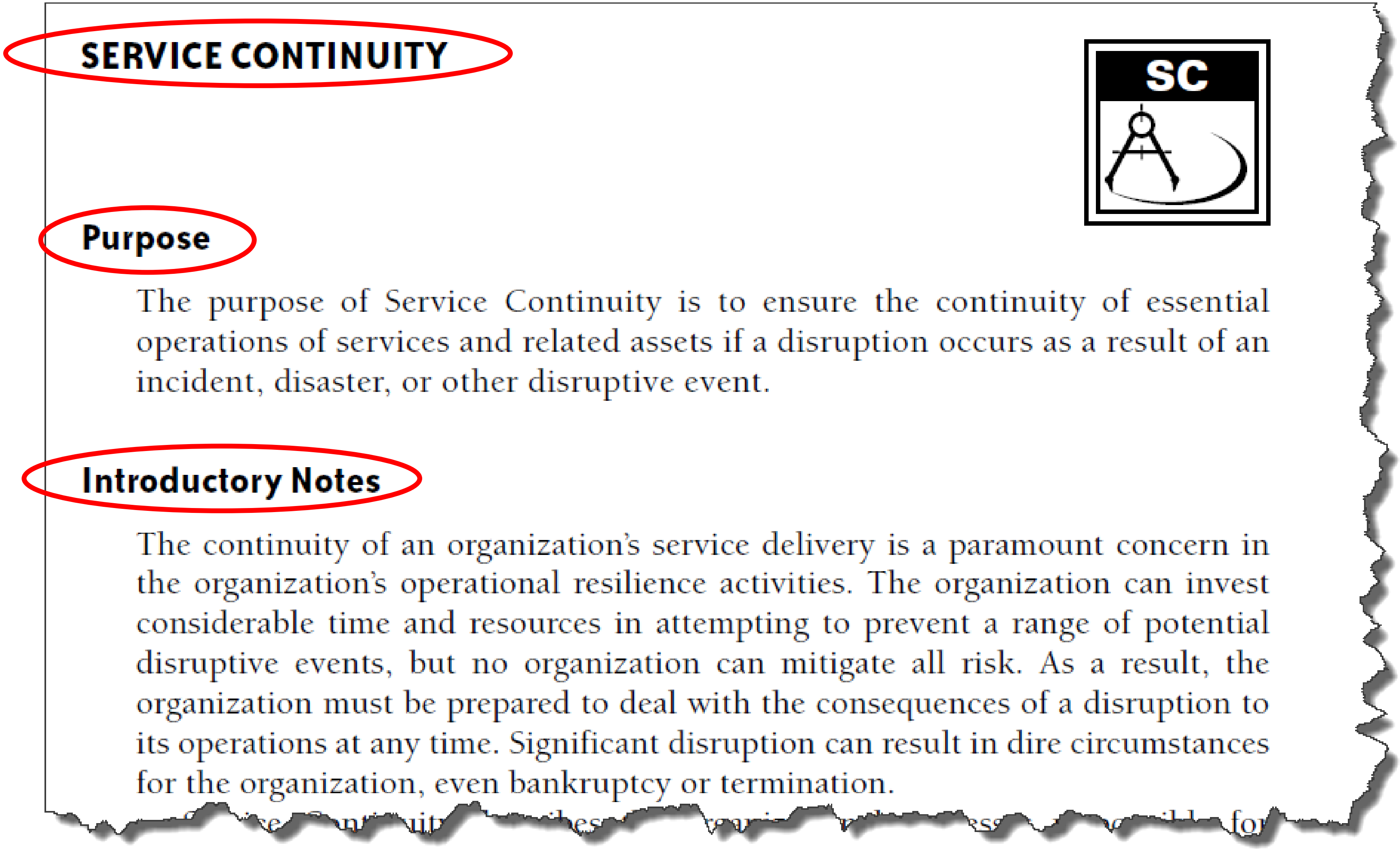
- Practices support goal achievement
- A suggested way to meet the goal

Activities that ensure the processes associated with the PA will be effective, repeatable, and lasing

Example: Service Continuity Process Area

- Access Management
- Asset Definition and Management
- Communications
- Compliance
- Controls Management
- Enterprise Focus
- Environmental Control
- External Dependencies
- Financial Resource Management
- Human Resource Management
- Identity Management
- Incident Management & Control
- Knowledge & Information Mgmt
- Measurement and Analysis
- Monitoring
- Organizational Process Focus
- Organizational Process Definition
- Organizational Training & Awareness
- People Management
- Resilience Requirements Development
- Resilience Requirements Management
- Resilient Technical Solution Engr.
- Risk Management
- Service Continuity
- Technology Management
- Vulnerability Analysis & Resolution

Example: Service Continuity Process Area



SERVICE CONTINUITY

SC

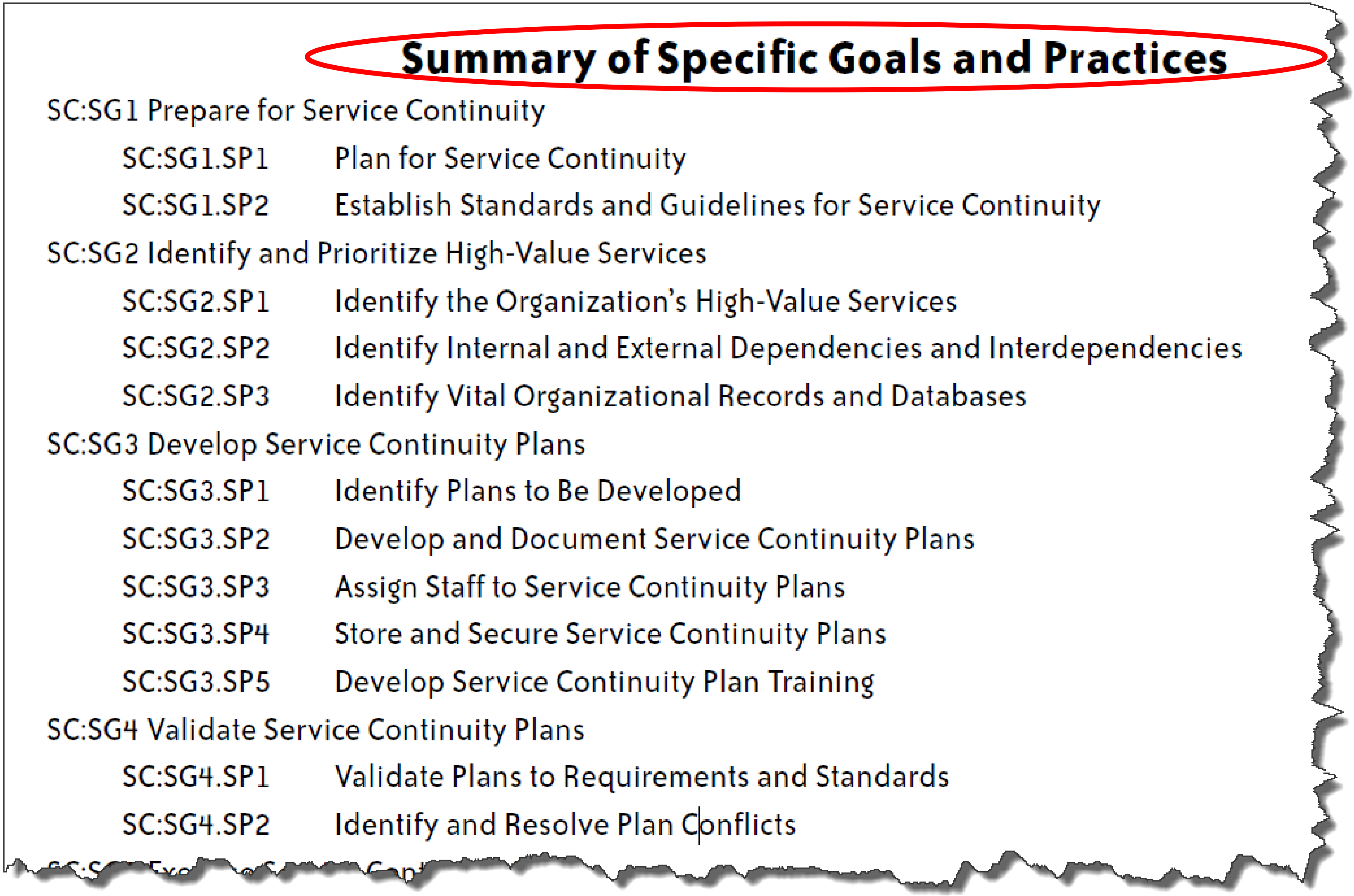
Purpose

The purpose of Service Continuity is to ensure the continuity of essential operations of services and related assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Introductory Notes

The continuity of an organization's service delivery is a paramount concern in the organization's operational resilience activities. The organization can invest considerable time and resources in attempting to prevent a range of potential disruptive events, but no organization can mitigate all risk. As a result, the organization must be prepared to deal with the consequences of a disruption to its operations at any time. Significant disruption can result in dire circumstances for the organization, even bankruptcy or termination.

Example: Service Continuity Process Area



Summary of Specific Goals and Practices

SC:SG1 Prepare for Service Continuity

- SC:SG1.SP1 Plan for Service Continuity
- SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity

SC:SG2 Identify and Prioritize High-Value Services

- SC:SG2.SP1 Identify the Organization’s High-Value Services
- SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies
- SC:SG2.SP3 Identify Vital Organizational Records and Databases

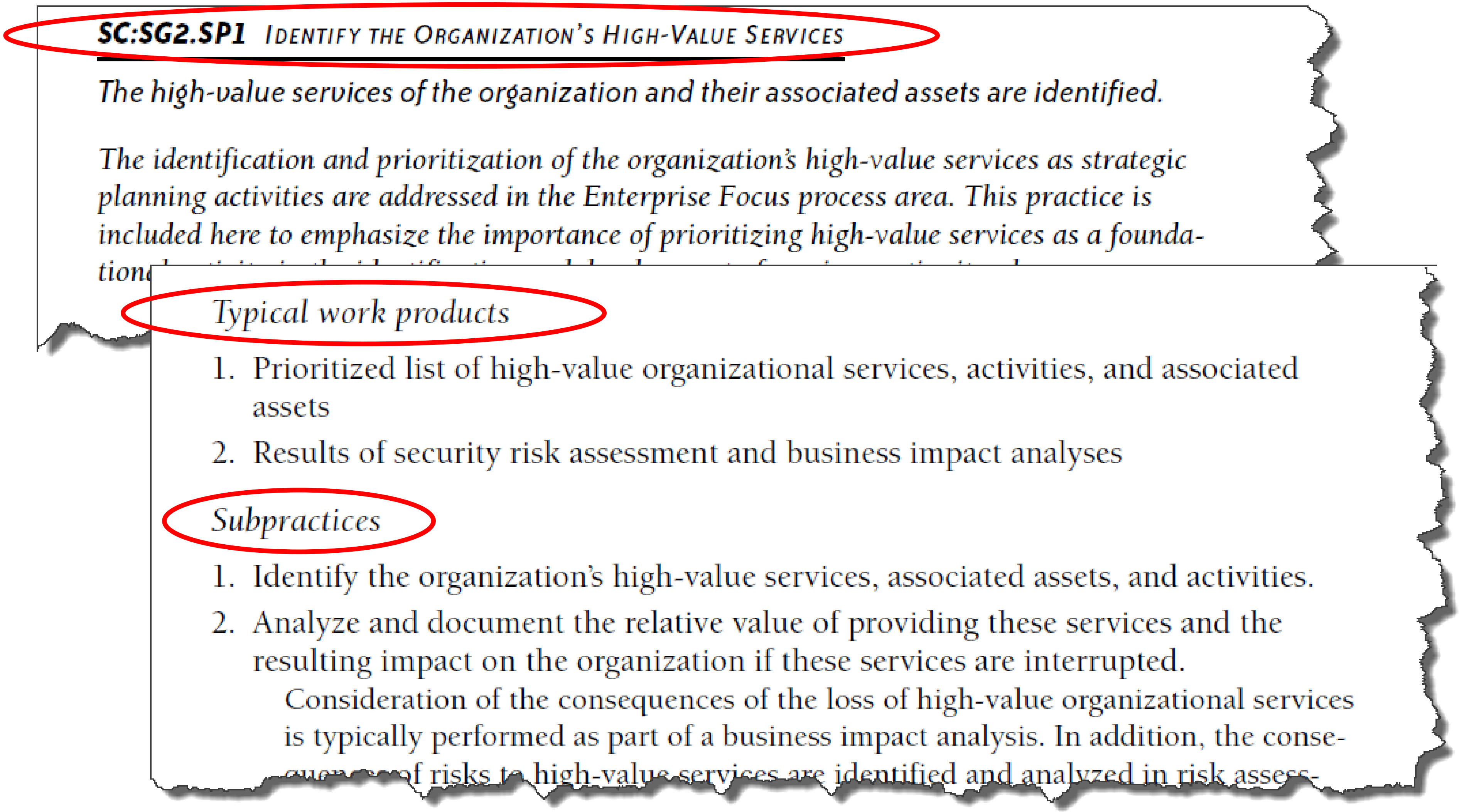
SC:SG3 Develop Service Continuity Plans

- SC:SG3.SP1 Identify Plans to Be Developed
- SC:SG3.SP2 Develop and Document Service Continuity Plans
- SC:SG3.SP3 Assign Staff to Service Continuity Plans
- SC:SG3.SP4 Store and Secure Service Continuity Plans
- SC:SG3.SP5 Develop Service Continuity Plan Training

SC:SG4 Validate Service Continuity Plans

- SC:SG4.SP1 Validate Plans to Requirements and Standards
- SC:SG4.SP2 Identify and Resolve Plan Conflicts

Example: Service Continuity Process Area



SC:SG2.SP1 IDENTIFY THE ORGANIZATION'S HIGH-VALUE SERVICES

The high-value services of the organization and their associated assets are identified.

The identification and prioritization of the organization's high-value services as strategic planning activities are addressed in the Enterprise Focus process area. This practice is included here to emphasize the importance of prioritizing high-value services as a founda-tion

Typical work products

1. Prioritized list of high-value organizational services, activities, and associated assets
2. Results of security risk assessment and business impact analyses

Subpractices

1. Identify the organization's high-value services, associated assets, and activities.
2. Analyze and document the relative value of providing these services and the resulting impact on the organization if these services are interrupted.

   Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the conse-quences of risks to high-value services are identified and analyzed in risk assess-

RMM Process Areas

- Access Management
- Asset Definition and Management
- Communications
- Compliance
- Controls Management
- Enterprise Focus
- Environmental Control
- External Dependencies
- Financial Resource Management
- Human Resource Management
- Identity Management
- Incident Management & Control
- Knowledge & Information Mgmt

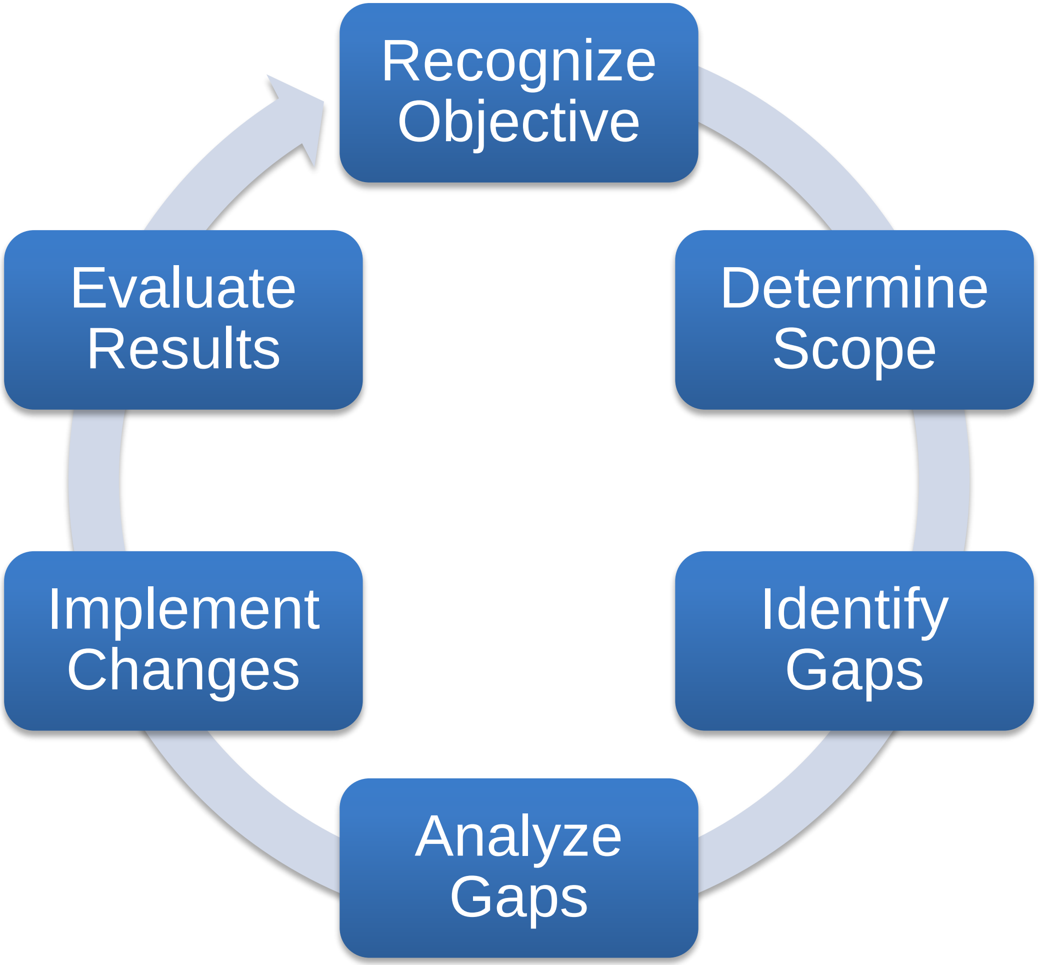
- Measurement and Analysis
- Monitoring
- Organizational Process Focus
- Organizational Process Definition
- Organizational Training & Awareness
- People Management
- Resiliency Requirements Development
- Resiliency Requirements Management
- Resilient Technical Solution Engr.
- Risk Management
- Service Continuity
- Technology Management
- Vulnerability Analysis & Resolution

Using the Model

CERT-RMM can be used as a…

- Starting point for socializing convergence principles across security, business continuity, and IT operations activities
- Reference model for understanding the scope of managing operational resilience
- Taxonomy
- Organizing construct for codes of practice
- Process improvement model to catalyze a process improvement effort
- Baseline from which to appraise an organization’s capability
- Guide for improvement in areas where an organization’s capability does not equal its desired state
- Source of ideas and guidance for solving problems in the organization’s operation

Using CERT-RMM for Improvement



Recognize Objective

Determine Scope

Identify Gaps

Analyze Gaps

Implement Changes

Evaluate Results

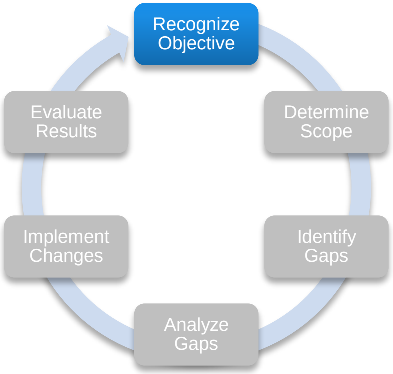
NOTE: Guidance for Putting it into Practice

Two sample (very different) scenarios for putting principles of operational resilience into practice:

1. A major and visible disruptive event has taken place and you want to apply concepts from his module to deal with it.
2. The there is a desire to put in place a strategic plan to raise the bar.

NOTE: Both are "improvement" activities.

Recognizing Objectives



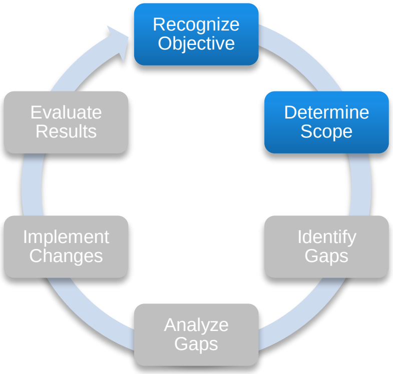
Objectives frame and provide context

Answer the question: *What are we trying to accomplish with the improvement effort?*

Typical themes:

- Are we doing all that we should to manage business continuity (or security, IT ops, or a combination)?
- How can we minimize the potential disruption from *<some known risk or category of risk>*?
- How can we improve the efficiency, effectiveness, or consistency of our operational risk management activities (security, BC, & IT ops)?
- Do our policies and guidelines produce the risk management activities that we want them to? How can we improve policy?

Determining Scope



Two elements:

- **Organizational scope:**
- On which part of the organization will we focus?
- **Model scope:**
- Which parts of the CERT-RMM will we use?
  - Whole process areas (1-6 typically)
  - Parts of process areas (a set of practices)

Both elements should align with objectives and sponsorship

Model scoping can be easily accomplished by walking the model outline in a small workshop or meeting

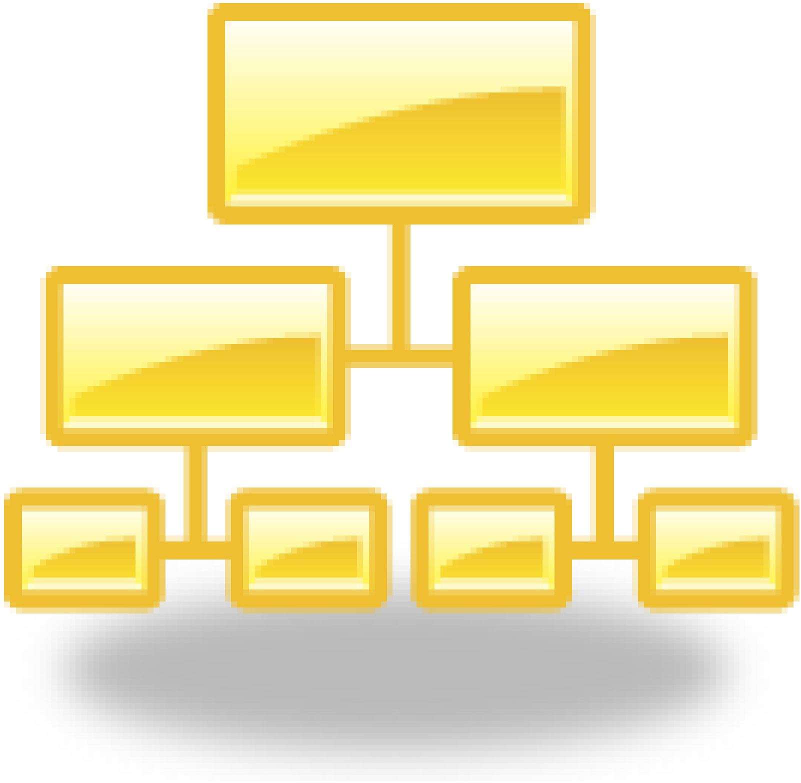
Organizational Scope

Determine Scope

Where, in the organization, process improvement will be focused

Must consider

- Span of sponsorship developed in Initiating phase
- Span of authority of the improvement team
- Schedule feasibility for desired improvements
- Start small



Model Scope

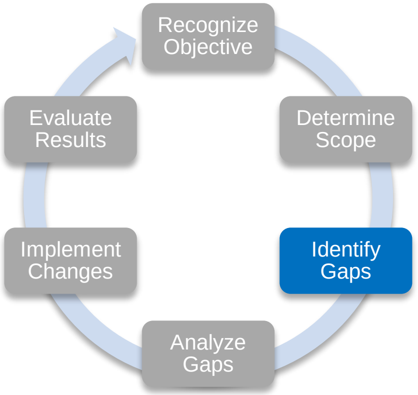
Determine Scope

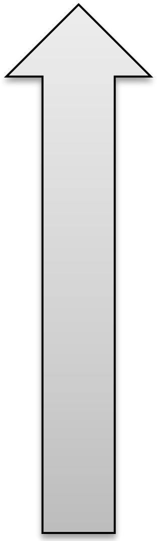
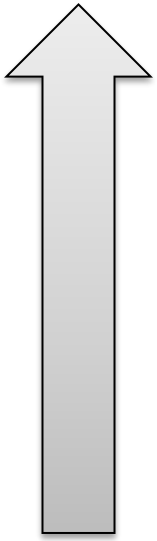
Determines which areas of the model will be selected for process improvement

When selecting, consider process areas that

- May be causing “pain” or perceived weakness
- Align with regulatory or industry initiatives and objectives
- Align with organizational objectives or initiatives
- Support other organizational process improvement initiatives such as Six Sigma or ITIL
- Explore areas in which the organization needs to develop competency

Identifying Gaps



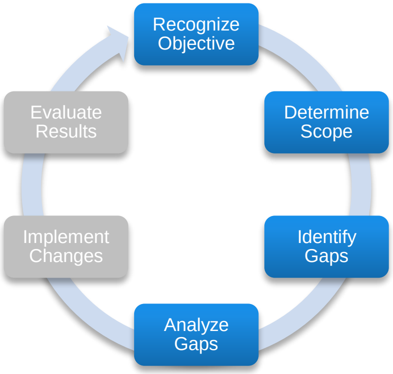
Formality	Complexity	Methodology
Formal  Informal	Rigorous  Lightweight	**CERT-RMM Capability Appraisals (CAM)** • Outputs include detailed practice-level characterizations and written findings statements • Different degrees of rigor • Adapted from CMMI SCAMPI methods
		Questionnaire-based gap analysis • Examples: CRR, ES-C2M2
		Gap Analysis Roundtable or Workshop • Assemble a group of internal experts • Informally evaluate the organization’s implementation of the model practices in a roundtable or workshop setting

CERT-RMM Appraisal Comparison

Identify Gaps

		Class A	Class B	Class C
Model-Related Outputs	Process Area	Capability Level Ratings (0, 1, 2, or 3)	--	--
	Specific Goals Generic Goals	Goal Ratings (Satisfied or Not Satisfied)	--	--
	Specific Practices Generic Practices	Characterization of implementation on 5-point scale (Fully, Largely, Partially, Not, Not Yet Implemented) Findings statements (strengths & weaknesses)	Characterization of approach on 3-point scale (High, medium, low) Statements (strength/weakness)	Characterization of intent on 3-point scale (High, medium, low) Statements (strength/weakness)
Effort	Appraisal team:	4 or more	2 or more	1 or more
	Depth of investigation:	High	Medium	Low
	Resource requirements:	High	Medium	Low

Analyzing Gaps

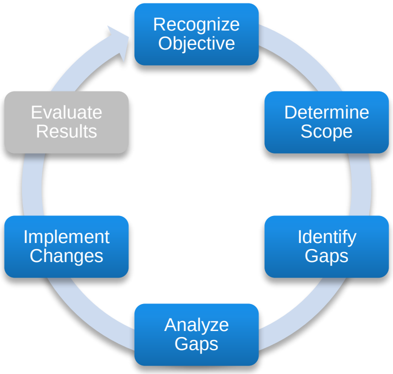


To make sure that closing gaps makes sense gaps should be analyzed:

- Is the cost for closing a gap worth the investment?
- Are there any efficiencies that can be realized by making the changes to close one or more gaps (efficiencies may include streamlining controls or compliance activities)?
- Which gaps are most important in the context of the objective?
- Are the organizational changes necessary to close the gaps within the bounds of sponsorship?

Output is a set of prioritized gaps to be closed

Implementing Changes

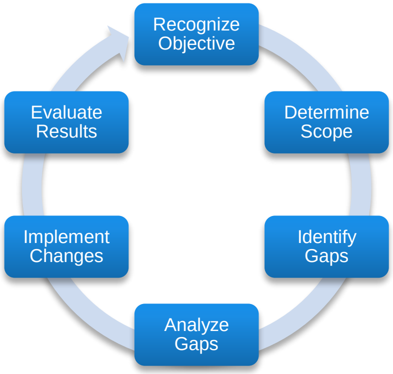


Use model guidance

- Subpractices and other informative material provide implementation guidance
- Code of Practice Crosswalk highlights connections between CERT-RMM and relevant standards and codes of practice, which can serve as additional implementation guidance
- Generic practices in the model provide guidance for having the changes persist in the organization

Consider measurements that could be implemented with the changes to help monitor results and inform management

Evaluating Results



Did we achieve the objective?

Did the changes stick? Can we be sure the new state will persist?

Are additional needs or objectives now apparent?

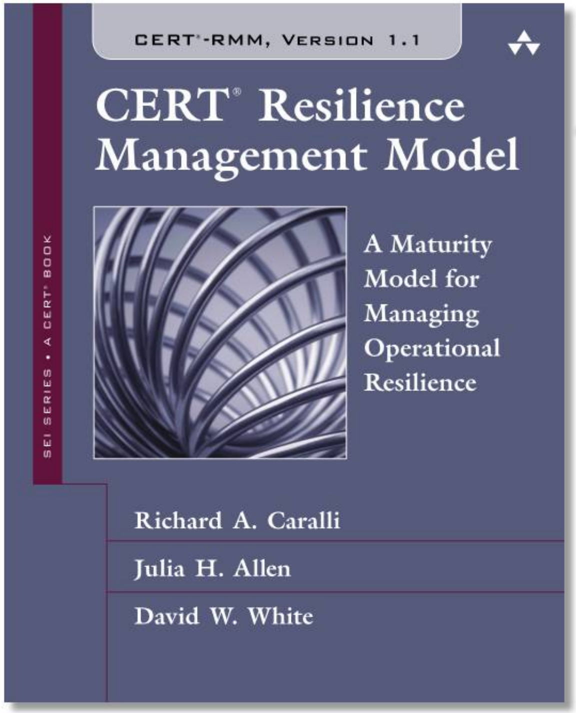
When should we make another improvement cycle?

If measurements were implemented, are they revealing desired trends?

Step-By-Step / Checklist / Roadmap …..

- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment.
- ❑ What are your operational risks? Who will be affected if there are realized?
- ❑ What hurdles do you face to effective operational resilience management?
- ❑ What operational risk management activates (silos) exist? Are there opportunities for convergence of some sort?
- ❑ Draw the resilience context diagram for your organization.
- ❑ What are your resilience requirement categories?
- ❑ Repeat the exercise for your organization.
- ❑ Select an process improvement cycle? Do you already use one?

CERT Resilience Management Model (CERT-RMM)



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI Series • A CERT® Book

Richard A. Caralli

Julia H. Allen

David W. White

http://www.cert.org/resilience/

Framework for managing and improving operational resilience

"…an extensive super-set of the things an organization could do to be more resilient."

- CERT-RMM adopter

For Managing Disaster Recovery, COOP, Business Continuity Policies

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

For FISMA Compliance

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

For Managing Cloud Computing

- Access Management
- Asset Definition and Management
- Communications
- Compliance
- Controls Management
- Enterprise Focus
- Environmental Control
- External Dependencies
- Financial Resource Management
- Human Resource Management
- Identity Management
- Incident Management & Control
- Knowledge & Information Mgmt

- Measurement and Analysis
- Monitoring
- Organizational Process Focus
- Organizational Process Definition
- Organizational Training & Awareness
- People Management
- Resiliency Requirements Development
- Resiliency Requirements Management
- Resilient Technical Solution Engr.
- Risk Management
- Service Continuity
- Technology Management
- Vulnerability Analysis & Resolution

For Managing the Insider Threat Challenge

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

Step-By-Step / Checklist / Roadmap …..

- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment.
- ❑ What are your operational risks? Who will be affected if there are realized?
- ❑ What hurdles do you face to effective operational resilience management?
- ❑ What operational risk management activates (silos) exist? Are there opportunities for convergence of some sort?
- ❑ Draw the resilience context diagram for your organization.
- ❑ What are your resilience requirement categories?
- ❑ Repeat the exercise for your organization.
- ❑ Select an process improvement cycle? Do you already use one?
- ❑ Select a sample problem at your organization and do a model scoping exercise.

Summary of CERT-RMM

Distinguishing Features of RMM

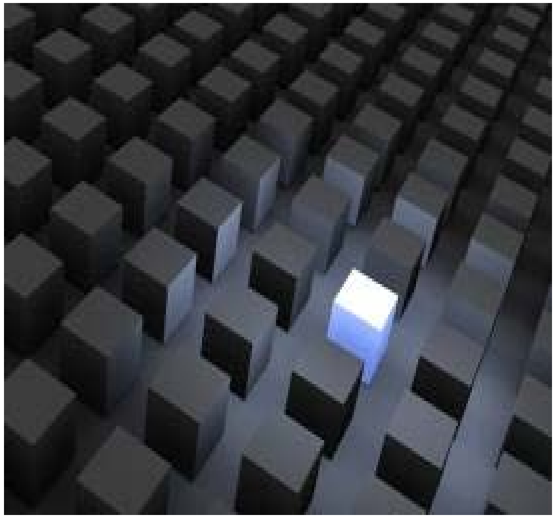
Converges key operational risk management activities: security, BC/DR, and IT operations

Guides **implementation and management** of operational resilience activities

Descriptive rather than prescriptive - focuses on the “what” not the “how”

Provides an organizing convention for effective selection and deployment of codes of practice and standards

Guide for improvement in areas where an organization’s capability does not equal its desired state



Distinguishing Features of RMM (Cont.)

Improves confidence in how an organization responds in times of operational stress

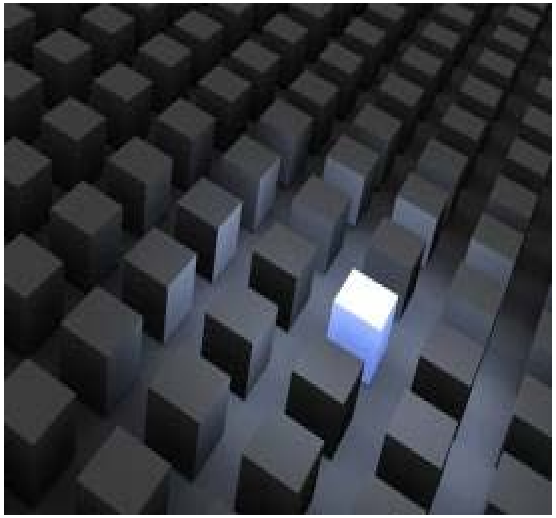
Baseline from which to perform an appraisal

Enables **measurements** of effectiveness

Process improvement model

Enables **institutionalization**

Not a proprietary model



Variety of Ways to Use RMM

Starting point for **socializing** important harmonization and **convergence** principles across security, business continuity, and IT operations activities

Reference model for understanding the scope of managing operational Resilience

Process improvement model to catalyze a process improvement effort

Baseline from which to perform an appraisal of an organization's capability

Guide for improvement in areas where an organization's capability does not equal its desired state

Organizing construct for codes of practice

Taxonomy

Proven Use Cases & Real Life Samples

- Success stories
- How are organizations utilizing the converged approaches?
- Who is actually utilizing and benefiting from CERT-RMM?

Who is using CERT-RMM?

Working with CERT

Carnegie Mellon University

Discover Financial

Highlands Union Bank

Lockheed Martin Corporation

Marshall & Ilsley Corporation

PNC Corporation

University of Pittsburgh Medical Center

US Dept of Energy

US Dept of Homeland Security

US Dept of Health & Human Services

US Environmental Protection Agency

US National Security Agency

US Postal Inspection Service

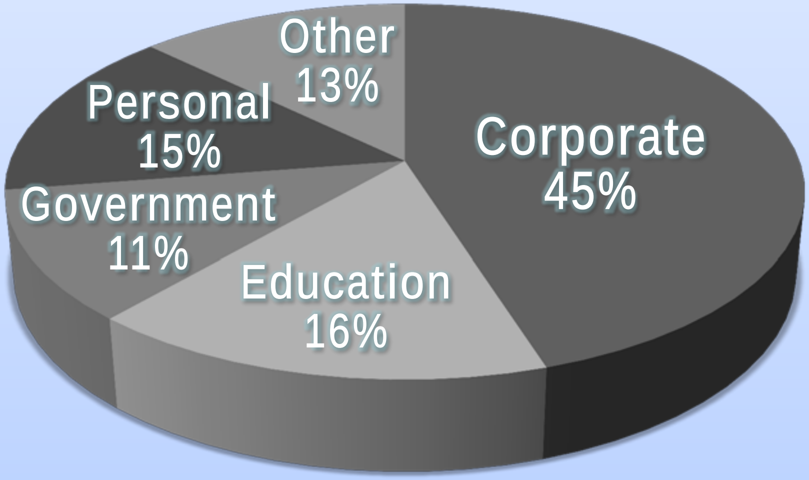
USBank

SunGard

Etc…

Independently

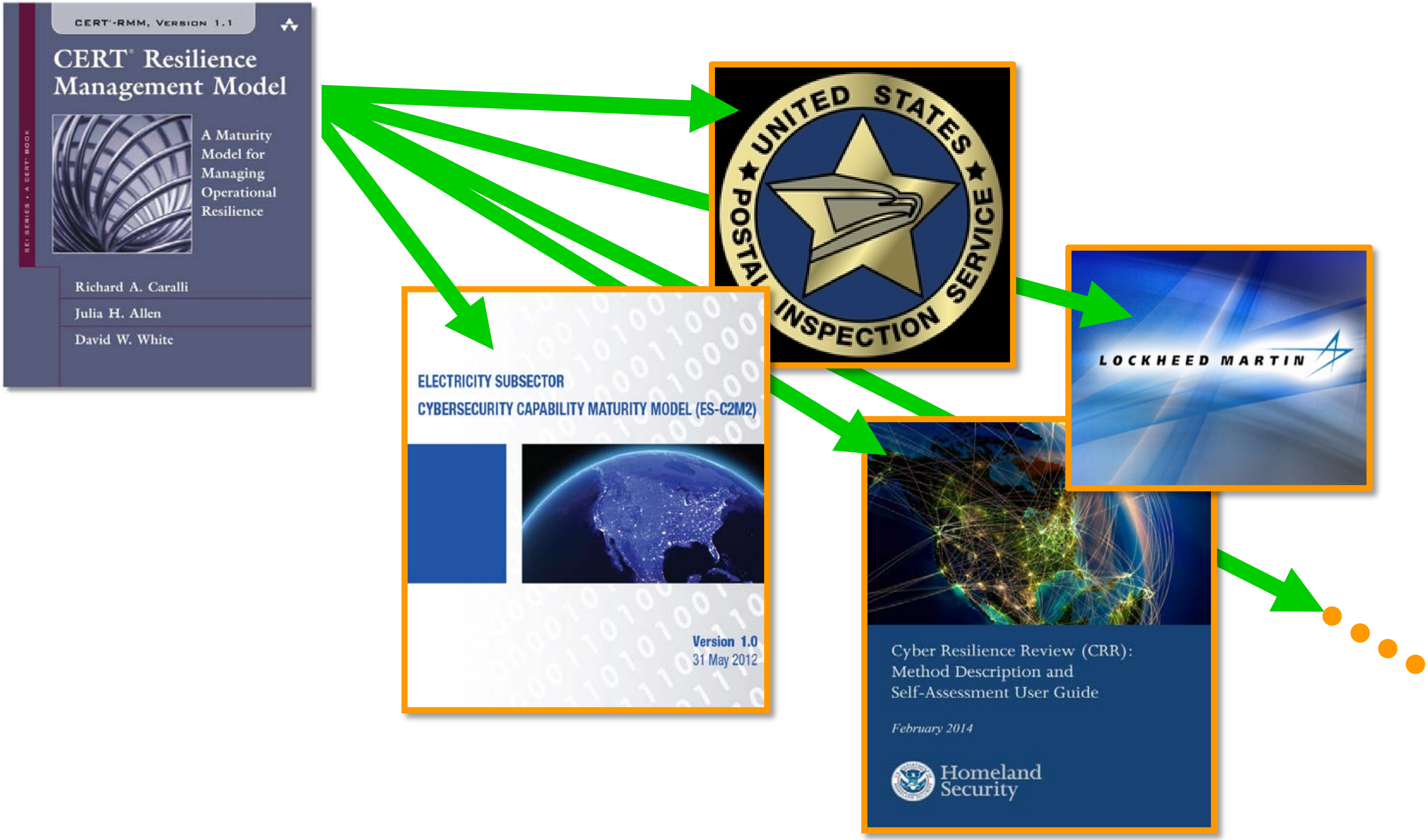
CERT-RMM v1.0: more than 3000 downloads:



Organization type reported on download

CERT-RMM v1.1 (published by Addison-Wesley) in second printing

A Sampling of CERT-RMM Applications and Derivatives



CERT®-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

SEI Series • A CERT® Book

Richard A. Caralli

Julia H. Allen

David W. White

ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0

31 May 2012

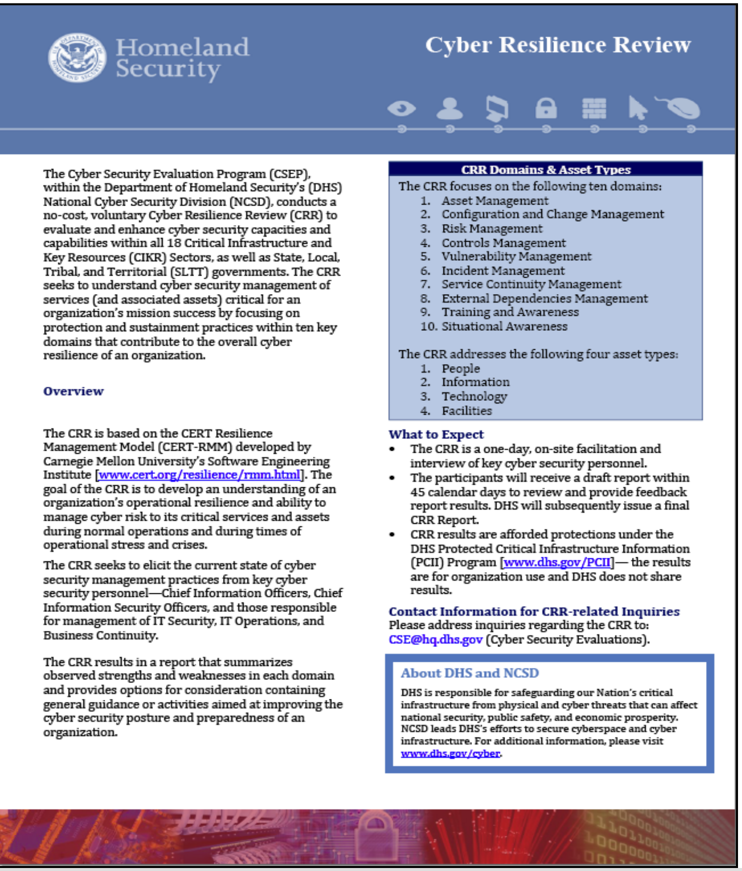
Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide

February 2014

Homeland Security

CYBER RESILIENCE REVIEW

US Department of Homeland Security Cyber Resilience Review (CRR) Program



Homeland Security

Cyber Resilience Review

The Cyber Security Evaluation Program (CSEP), within the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD), conducts a no-cost, voluntary Cyber Resilience Review (CRR) to evaluate and enhance cyber security capacities and capabilities within all 18 Critical Infrastructure and Key Resources (CIKR) Sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments. The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization.

Overview

The CRR is based on the CERT Resilience Management Model (CERT-RMM) developed by Carnegie Mellon University's Software Engineering Institute [www.cert.org/resilience/rmm.html]. The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services and assets during normal operations and during times of operational stress and crises.

The CRR seeks to elicit the current state of cyber security management practices from key cyber security personnel—Chief Information Officers, Chief Information Security Officers, and those responsible for management of IT Security, IT Operations, and Business Continuity.

The CRR results in a report that summarizes observed strengths and weaknesses in each domain and provides options for consideration containing general guidance or activities aimed at improving the cyber security posture and preparedness of an organization.

CRR Domains & Asset Types

The CRR focuses on the following ten domains:

1. Asset Management
2. Configuration and Change Management
3. Risk Management
4. Controls Management
5. Vulnerability Management
6. Incident Management
7. Service Continuity Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The CRR addresses the following four asset types:

1. People
2. Information
3. Technology
4. Facilities

What to Expect

- The CRR is a one-day, on-site facilitation and interview of key cyber security personnel.
- The participants will receive a draft report within 45 calendar days to review and provide feedback report results. DHS will subsequently issue a final CRR Report.
- CRR results are afforded protections under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/PCII]— the results are for organization use and DHS does not share results.

Contact Information for CRR-related Inquiries

Please address inquiries regarding the CRR to: CSE@hq.dhs.gov (Cyber Security Evaluations).

About DHS and NCSD

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. NCSD leads DHS's efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.

What is CRR?

The Cyber Resilience Review (CRR) is a review of the overall practice, **integration**, and health of an organization's cyber security program.

The CRR seeks to understand cyber security management of services **and associated assets critical for an organization's mission success**.

Focusing on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization.

CRR Goal

Develop an accurate and efficient method to characterize an organization's

- **operational resilience**, and
- ability to manage cyber risk to its critical services and its related assets **during normal operations and during times of stress and crisis**

The CRR is based on CERT-RMM.

Developed for DHS

Target organizations

Critical Infrastructure and Key Resources (CIKR) providers

State, Local, Tribal, and Territorial (SLTT) governments

> ***"… Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters …"***

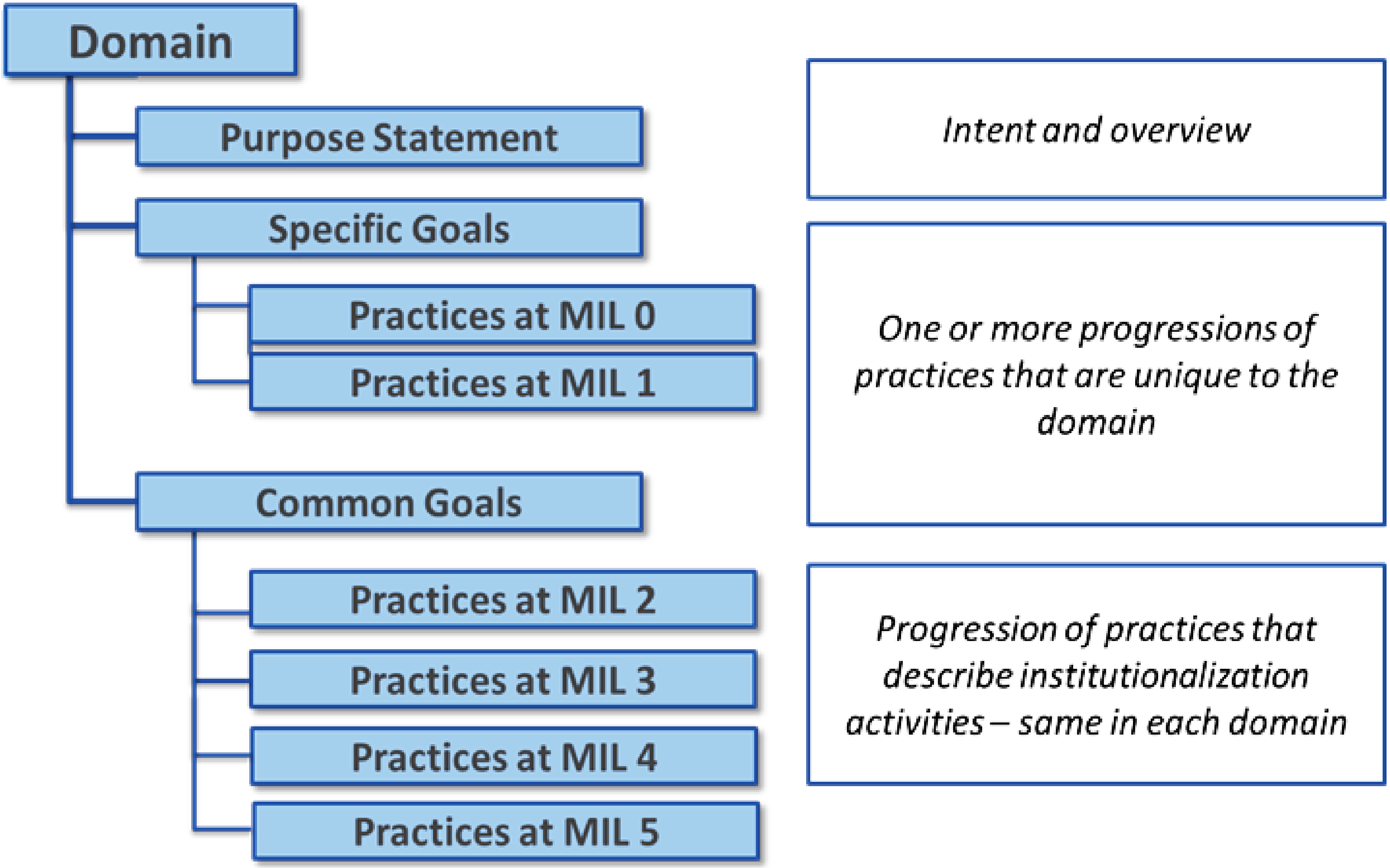
CRR Domains

The ten domains in CRR represent important areas that contribute to the cyber resilience of an organization.

The domains focus on practices an organization should have in place to **assure the protection and sustainment of its critical service**.

CRR Domains	
AM	Access Management
CTL	Controls Management
CCM	Configuration and Change Management
VM	Vulnerability Management
IM	Incident Management
SCM	Service Continuity Management
RM	Risk Management
EXD	External Dependencies Management
TA	Training and Awareness
SA	Situational Awareness

CRR Domain Structure



Domain

Purpose Statement

Specific Goals

Practices at MIL 0

Practices at MIL 1

Common Goals

Practices at MIL 2

Practices at MIL 3

Practices at MIL 4

Practices at MIL 5

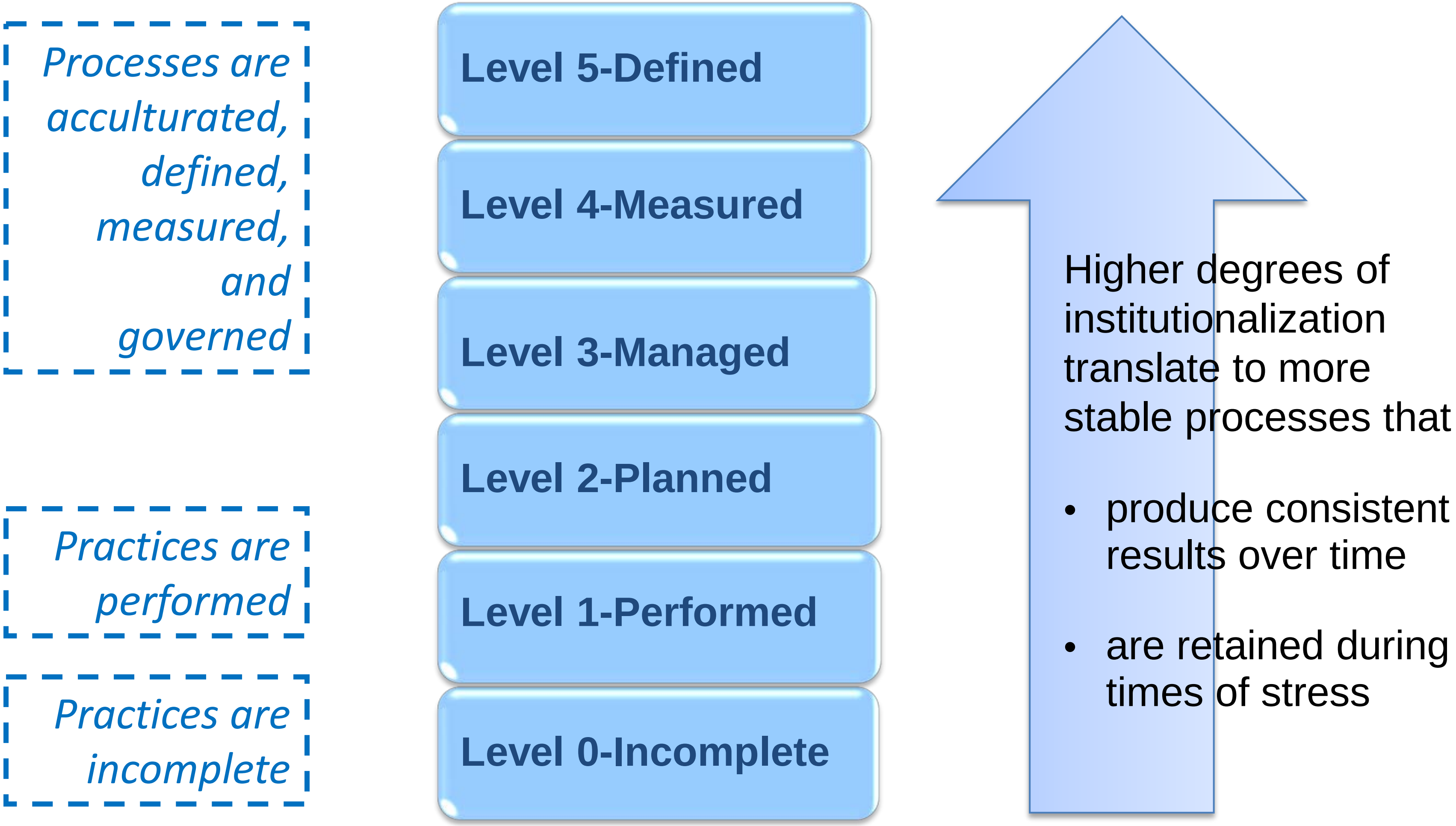
Intent and overview

One or more progressions of practices that are unique to the domain

Progression of practices that describe institutionalization activities – same in each domain

Process Institutionalization in the CRR

Maturity indictor levels (MIL) are used in CRR v2 to measure process institutionalization



Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete

Level 5-Defined

Level 4-Measured

Level 3-Managed

Level 2-Planned

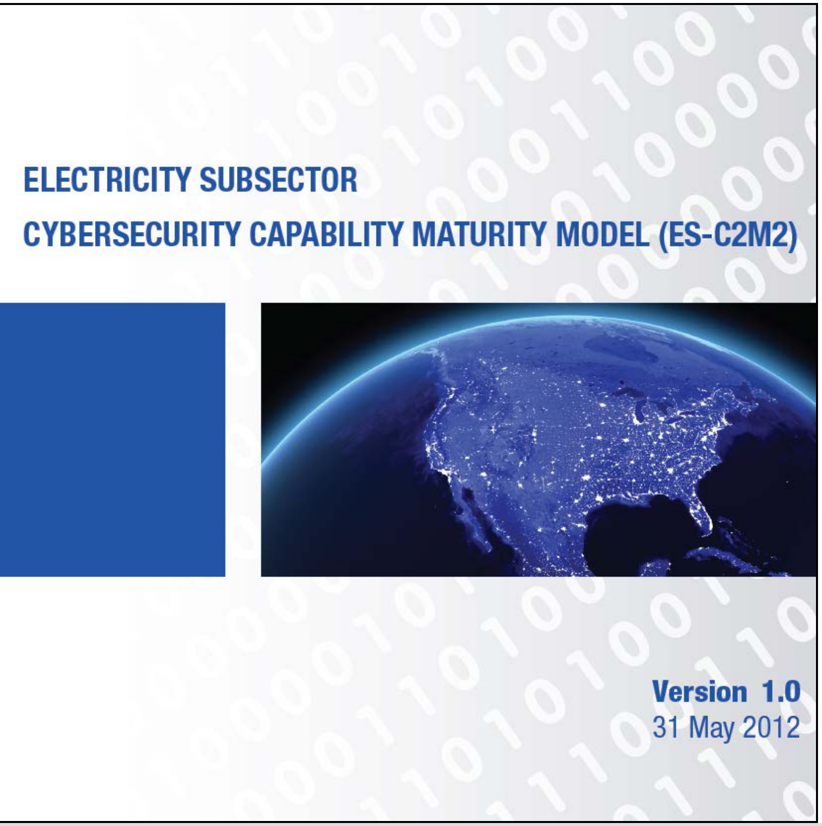
Level 1-Performed

Level 0-Incomplete

Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

US Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



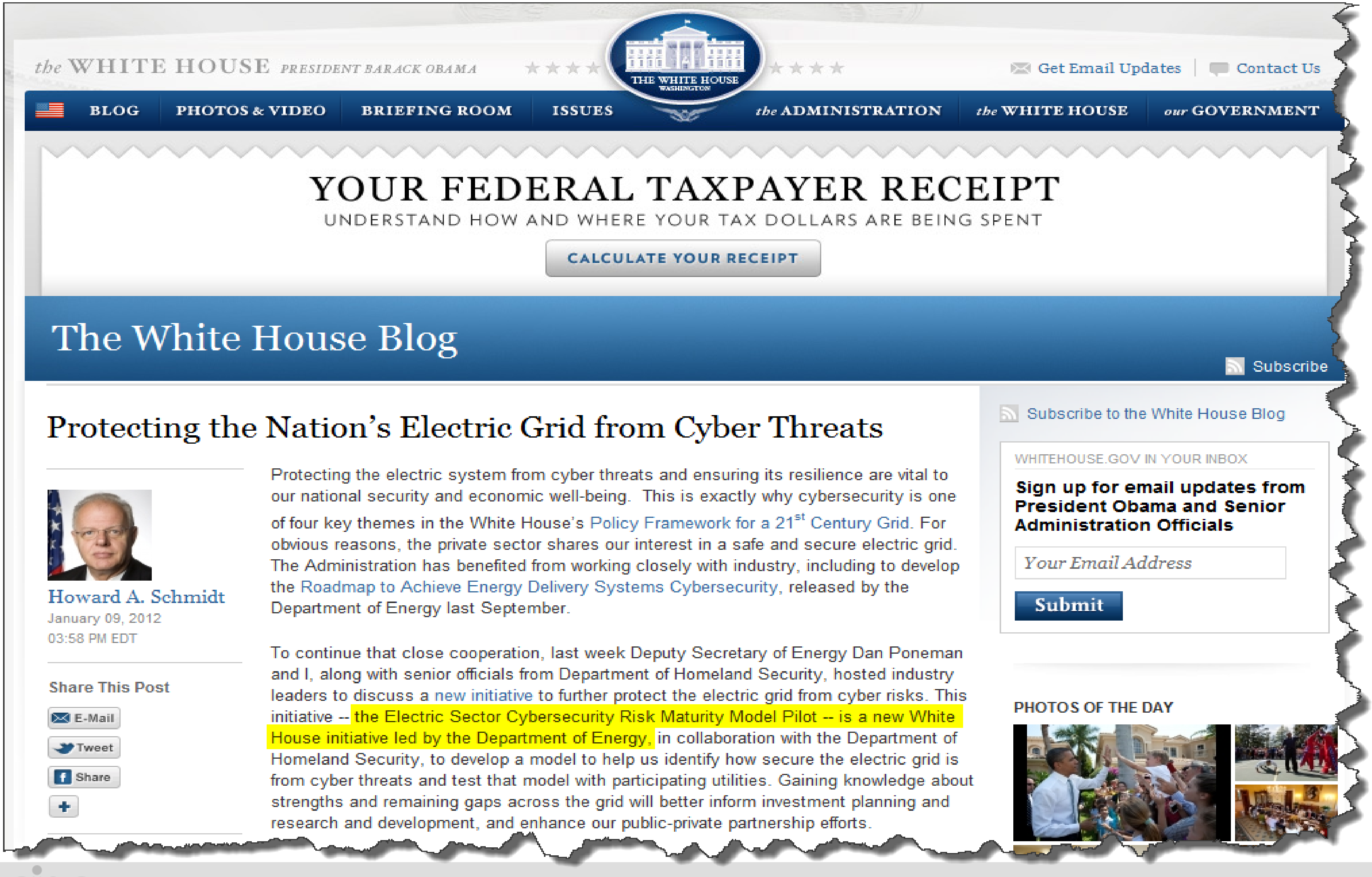
ELECTRICITY SUBSECTOR

CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0

31 May 2012

White House sponsorship



the WHITE HOUSE PRESIDENT BARACK OBAMA ★★★★ THE WHITE HOUSE WASHINGTON ★★★★ Get Email Updates | Contact Us

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRATION | the WHITE HOUSE | our GOVERNMENT

YOUR FEDERAL TAXPAYER RECEIPT

UNDERSTAND HOW AND WHERE YOUR TAX DOLLARS ARE BEING SPENT

CALCULATE YOUR RECEIPT

The White House Blog

Subscribe

Protecting the Nation's Electric Grid from Cyber Threats

Howard A. Schmidt
January 09, 2012
03:58 PM EDT

Share This Post

E-Mail
Tweet
Share
+

Protecting the electric system from cyber threats and ensuring its resilience are vital to our national security and economic well-being. This is exactly why cybersecurity is one of four key themes in the White House's Policy Framework for a 21st Century Grid. For obvious reasons, the private sector shares our interest in a safe and secure electric grid. The Administration has benefited from working closely with industry, including to develop the Roadmap to Achieve Energy Delivery Systems Cybersecurity, released by the Department of Energy last September.

To continue that close cooperation, last week Deputy Secretary of Energy Dan Poneman and I, along with senior officials from Department of Homeland Security, hosted industry leaders to discuss a new initiative to further protect the electric grid from cyber risks. This initiative -- the Electric Sector Cybersecurity Risk Maturity Model Pilot -- is a new White House initiative led by the Department of Energy, in collaboration with the Department of Homeland Security, to develop a model to help us identify how secure the electric grid is from cyber threats and test that model with participating utilities. Gaining knowledge about strengths and remaining gaps across the grid will better inform investment planning and research and development, and enhance our public-private partnership efforts.

Subscribe to the White House Blog

WHITEHOUSE.GOV IN YOUR INBOX

Sign up for email updates from President Obama and Senior Administration Officials

Your Email Address

Submit

PHOTOS OF THE DAY

ES-C2M2 Overview

Sponsor

- Department of Energy (DOE)

Target user organizations

- All electric utilities and grid operators, regardless of ownership structure, size, or function

Goal

- Develop capabilities to manage **dynamic threats** and understand cybersecurity posture of the grid

Objectives

- Strengthen cybersecurity capabilities
- Enable consistent evaluation and benchmarking of cybersecurity capabilities
- Share knowledge and best practices
- Enable prioritized actions and cybersecurity investments

What is ES-C2M2?

An organized set of cybersecurity practices

+

A self-evaluation questionnaire and scoring tool

=

For examining, benchmarking, and improving cybersecurity program

Developed by and for electric utilities, but proven useful for other types of organizations

ES-C2M2 domains

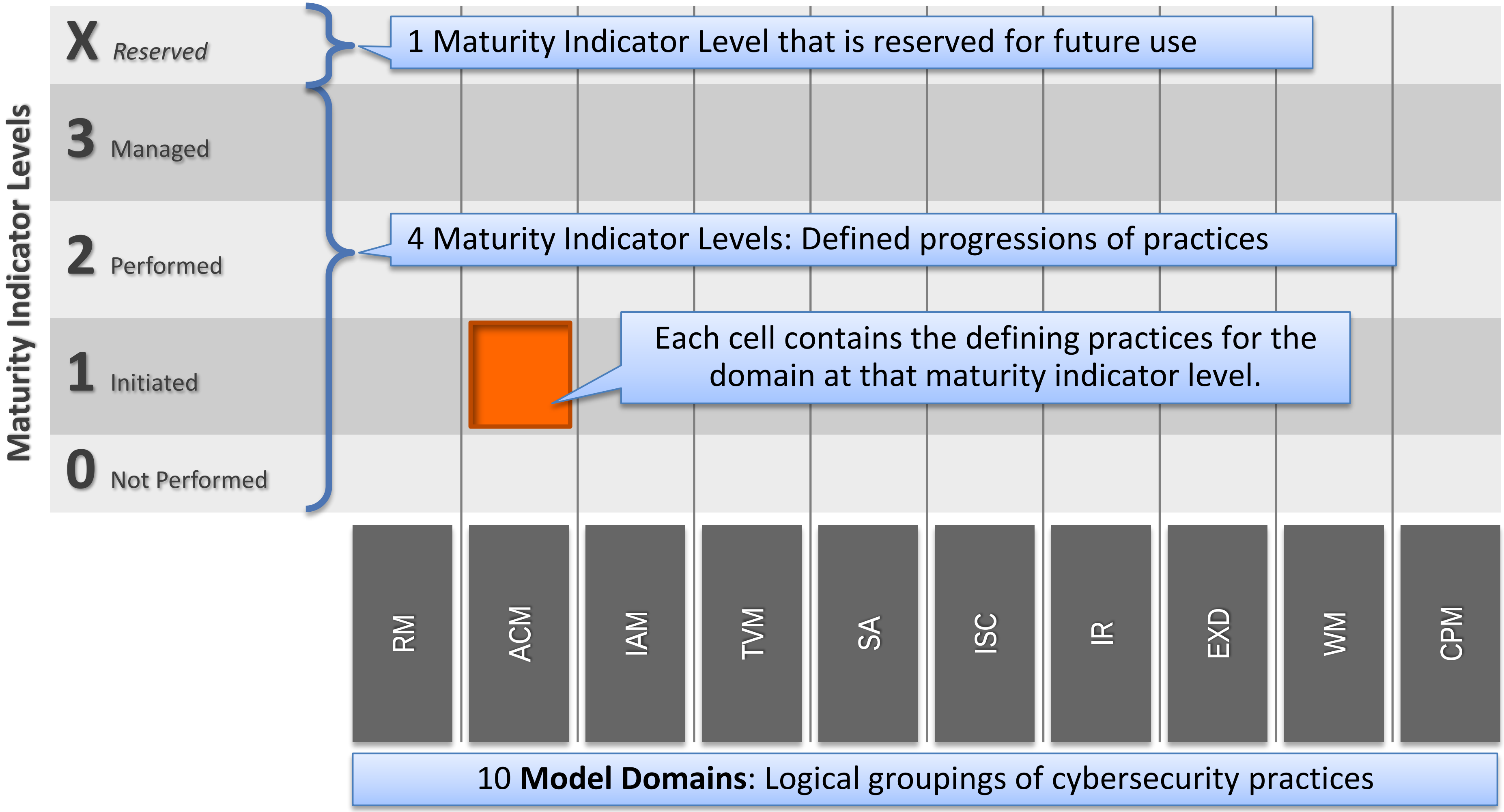
RISK	Risk Management
ASSET	Asset, Change, and Configuration Management
ACCESS	Identity and Access Management
THREAT	Threat and Vulnerability Management
SITUATION	Situational Awareness
SHARING	Information Sharing and Communications
RESPONSE	Event and Incident Response, Continuity of Operations
DEPENDENCIES	Supply Chain and External Dependencies Management
WORKFORCE	Workforce Management
CYBER	Cybersecurity Program Management

- **Domains are logical groupings of cybersecurity practices**
- **Each domain has a short name for easy reference**

ES-C2M2 Maturity Indicator Levels

Level	Name	Description
MIL0	Not Performed	• MIL1 has not been achieved in the domain
MIL1	Initiated	• Initial practices are performed, but may be ad hoc
MIL2	Performed	• Practices are documented • Stakeholders are involved • Adequate resources are provided for the practices • Standards or guidelines are used to guide practice implementation • Practices are more complete or advanced than at MIL1
MIL3	Managed	• Domain activities are guided by policy (or other directives) • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge • Practices are more complete or advanced than at MIL2

ES-C2M2 Structure



Maturity Indicator Levels

X *Reserved*

3 Managed

2 Performed

1 Initiated

0 Not Performed

1 Maturity Indicator Level that is reserved for future use

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level.

RM

ACM

IAM

TVM

SA

ISC

IR

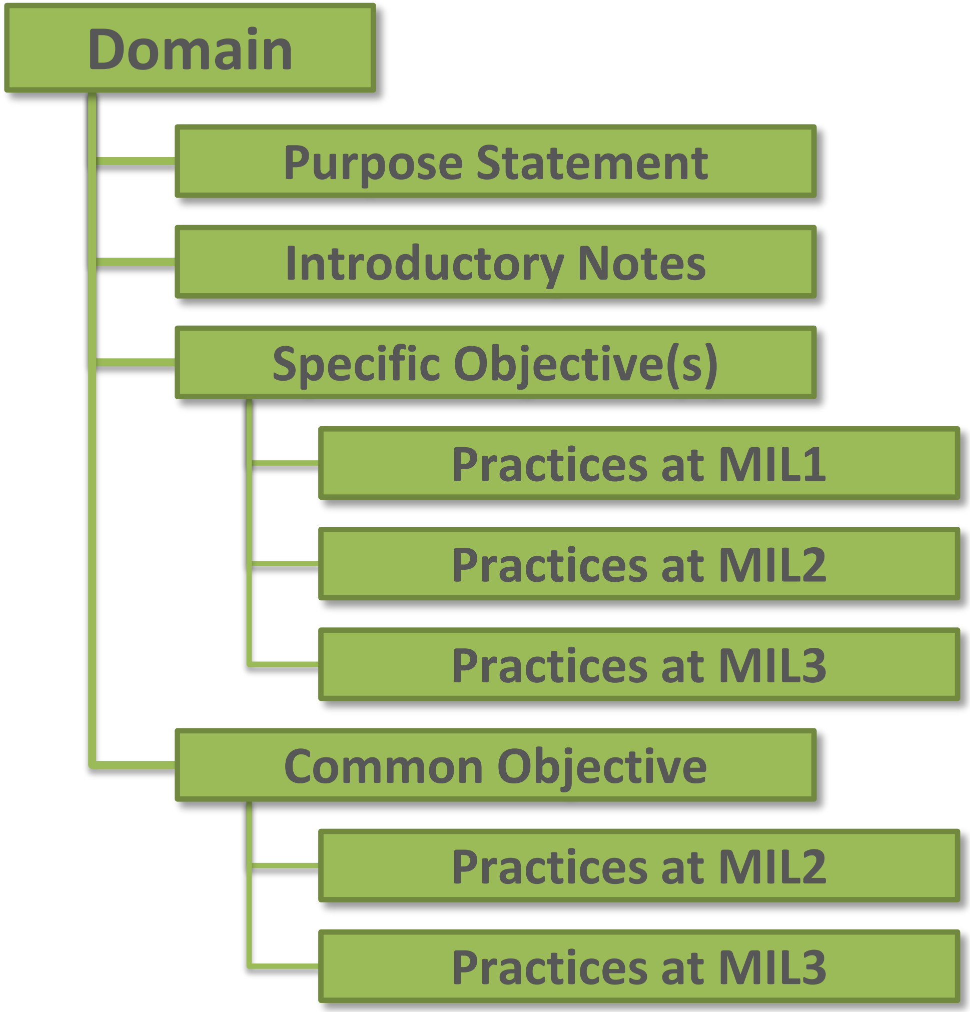
EXD

WM

CPM

10 **Model Domains**: Logical groupings of cybersecurity practices

Domain Structure



Domain

- Purpose Statement
- Introductory Notes
- Specific Objective(s)
  - Practices at MIL1
  - Practices at MIL2
  - Practices at MIL3
- Common Objective
  - Practices at MIL2
  - Practices at MIL3

Intent and overview

One or more progressions of practices that are unique to the domain

Progression of practices that describe institutionalization activities – same in each domain

Use of CERT-RMM by US Postal Inspection Service (USPIS)

UNITED STATES
POSTAL INSPECTION SERVICE
UNITED STATES POSTAL INSPECTION SERVICE
INSPECTOR
UNITED STATES

U.S. Postal Inspection Service (USPIS)

The law enforcement arm of the United States Postal Service

The oldest origins of any federal law enforcement agency in the United States dating back to 1772

Mission of the USPIS

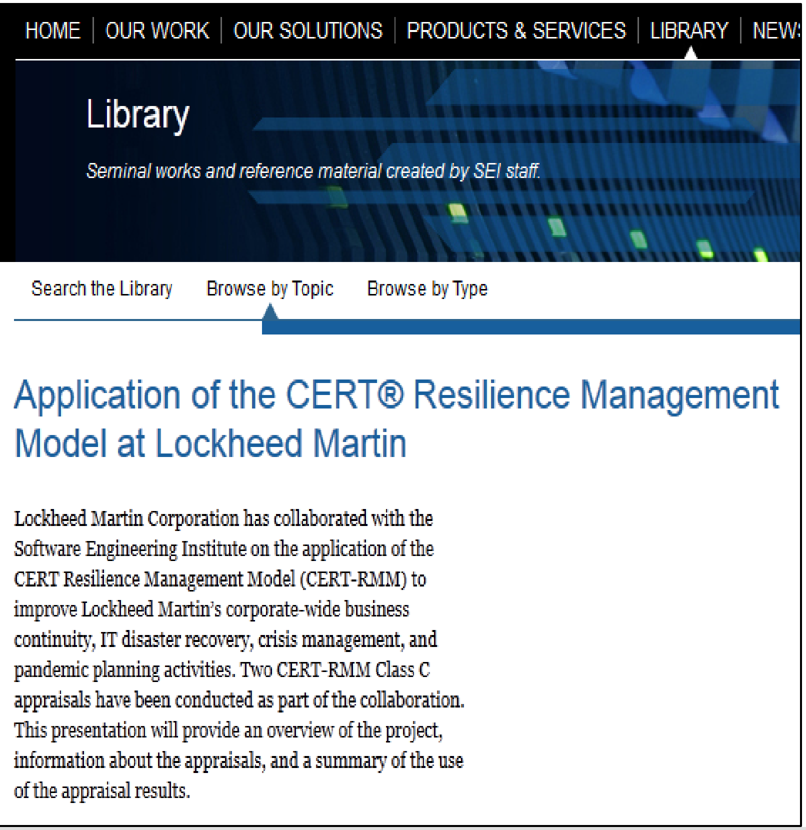
- Support and protect the U.S. Postal Service and its employees, infrastructure, and customers
- Enforce the laws that defend the nation’s mail system from illegal or dangerous use
- Ensure public trust in the mail

Use of CERT-RMM at USPIS

The USPIS has used CERT-RMM and its appraisal method to address

- export screening
- new product security
- measuring and monitoring risks associated with fraud
- physical security and aviation screening for international mail
- improved processes for investigative response to network security incidents
- development of mail-specific process areas for mail acceptance and revenue assurance

Lockheed Martin Corporation
Corporate Business Resilience Strategic Initiative


HOME | OUR WORK | OUR SOLUTIONS | PRODUCTS & SERVICES | LIBRARY | NEWS

Library

Seminal works and reference material created by SEI staff.

Search the Library
Browse by Topic
Browse by Type

Application of the CERT® Resilience Management Model at Lockheed Martin

Lockheed Martin Corporation has collaborated with the Software Engineering Institute on the application of the CERT Resilience Management Model (CERT-RMM) to improve Lockheed Martin's corporate-wide business continuity, IT disaster recovery, crisis management, and pandemic planning activities. Two CERT-RMM Class C appraisals have been conducted as part of the collaboration. This presentation will provide an overview of the project, information about the appraisals, and a summary of the use of the appraisal results.

LOCKHEED MARTIN

Uses of RMM at Lockheed Martin

To assess current level of competencies

- Where are we now? How good are we now?
- A consistent and common "ruler"
- Assessment by: self, internal 3rd party, external 3rd party

To guide future direction and investments

- Where do we want to be? How well do we want to get?
- Setting objectives
- Determining the investments required to reach the next/desired level

To measure progress towards the desired goal

Once the desired level is reached, to ensure that the plans and processes continue to evolve with the needs of the organization

- How do we stay there?

Uses of RMM at Lockheed Martin

Common business Resilience taxonomy and nomenclature

A reference model for our integrated business Resilience framework

To gauge the preparedness posture of individual business entities and/or the Enterprise as a whole in the areas of disaster recovery and business continuity

A mechanism to reveal insights about existing policies and guidelines

A guiding tool in the developing of new command media

A means to communicate key harmonization and convergence across business Resilience and information security

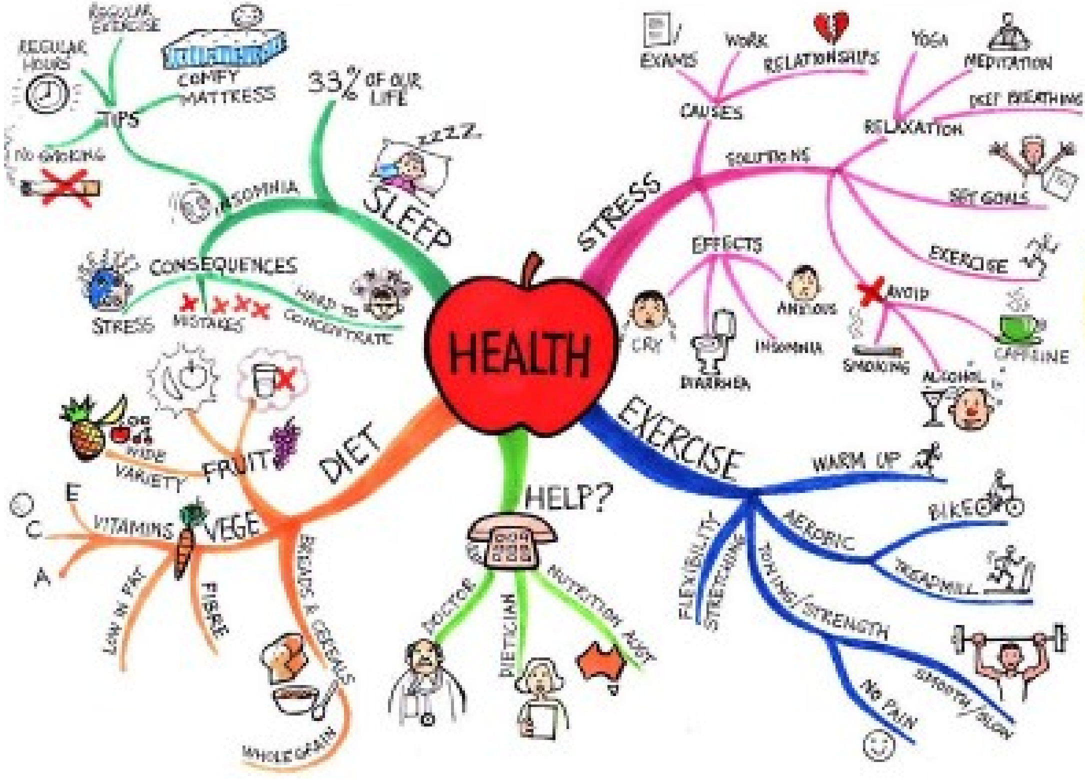
Challenges

Resilience Measurement

?

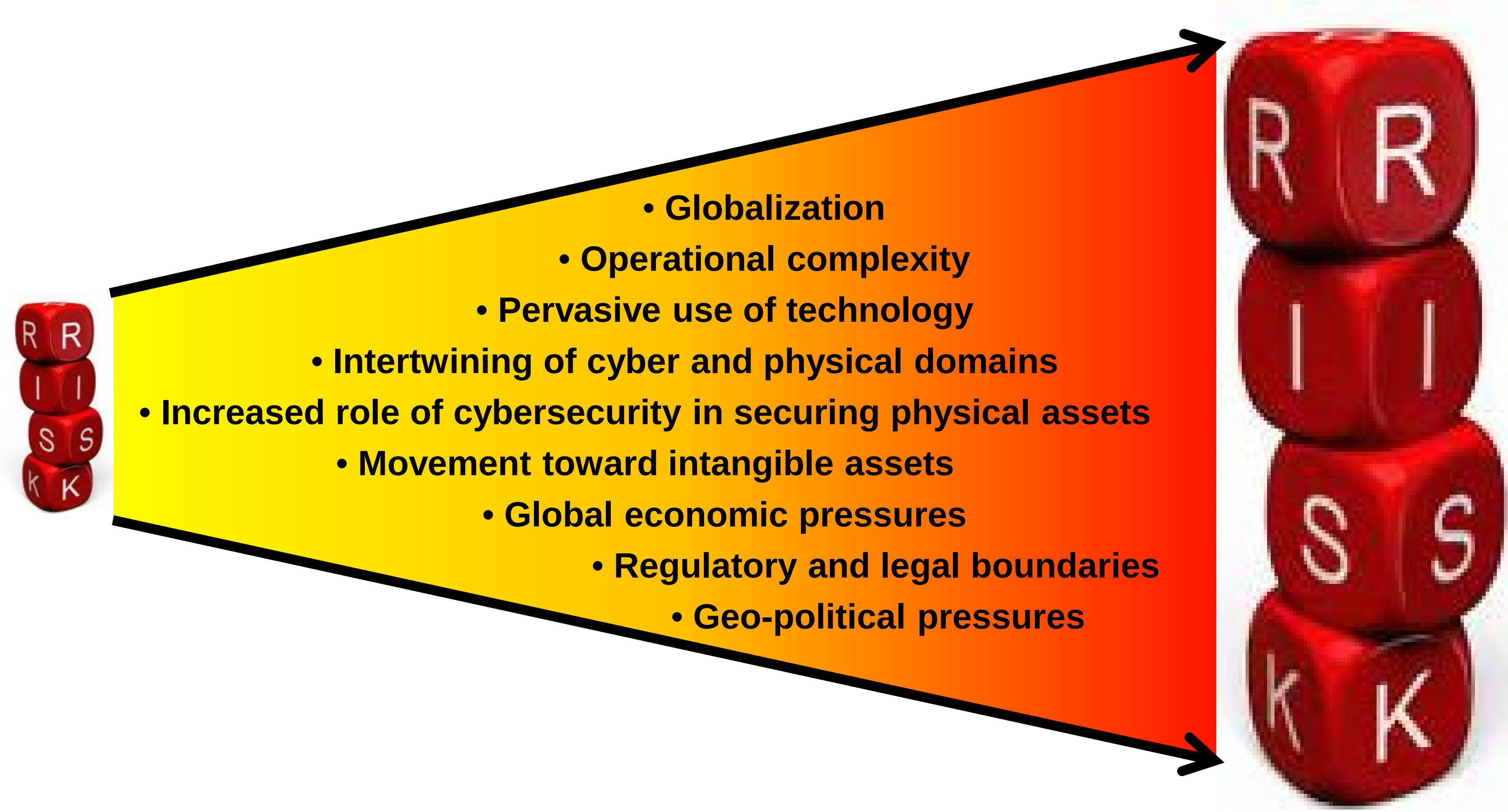
How do you measure an emergent property?

How have we been measuring health?



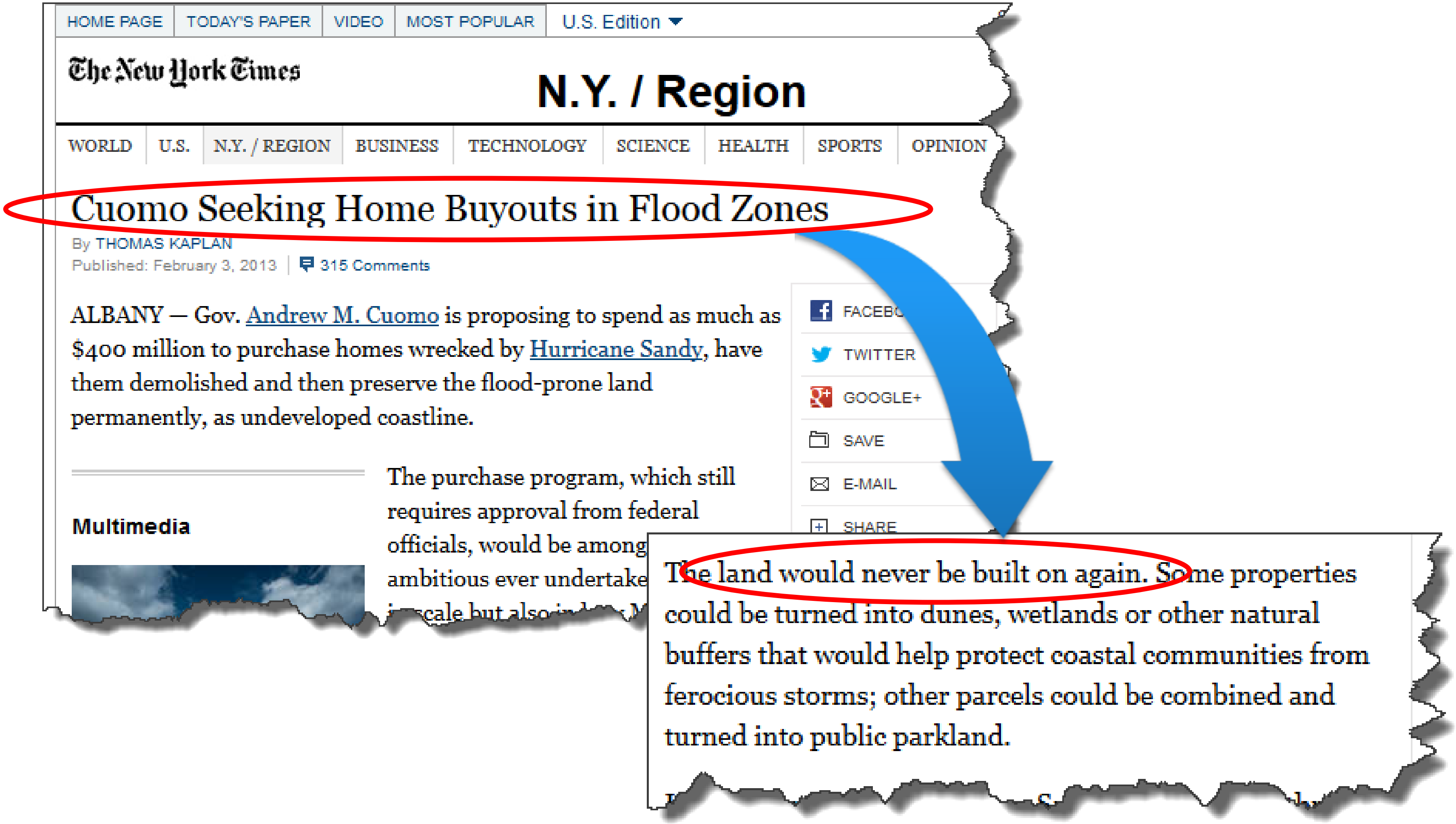
How have we been measuring health?

Should we keep “fighting” the risk landscape?



- Globalization
- Operational complexity
- Pervasive use of technology
- Intertwining of cyber and physical domains
- Increased role of cybersecurity in securing physical assets
- Movement toward intangible assets
- Global economic pressures
- Regulatory and legal boundaries
- Geo-political pressures

Re-Shaping (not fighting) the Risk Landscape?



Cuomo Seeking Home Buyouts in Flood Zones

By THOMAS KAPLAN
Published: February 3, 2013 | 315 Comments

ALBANY — Gov. Andrew M. Cuomo is proposing to spend as much as $400 million to purchase homes wrecked by Hurricane Sandy, have them demolished and then preserve the flood-prone land permanently, as undeveloped coastline.

The purchase program, which still requires approval from federal officials, would be among ambitious ever undertake in scale but also in

The land would never be built on again. Some properties could be turned into dunes, wetlands or other natural buffers that would help protect coastal communities from ferocious storms; other parcels could be combined and turned into public parkland.

Other Related Considerations

Next generation of integrated cyber-resilience management frameworks?

MODELS

Resilience Engineering – A new engineering discipline?

EDUCATION

RISK MGMT

Re-shaping (not fighting with) the risk landscape?

Should organizations be legally allowed to fight back when under cyber attack?

POLICY

Mechanisms to compose resilient systems from brittle components?

TECHNOLOGY

The hobbit
a brief summary
C'mon Bilbo... Let's adventure ... dragon... gold ... stuff
K.
Travelling + Adventure ...
Home now with me magic ring
END!
anythingcomic.com

Summary

Make a long-term commitment

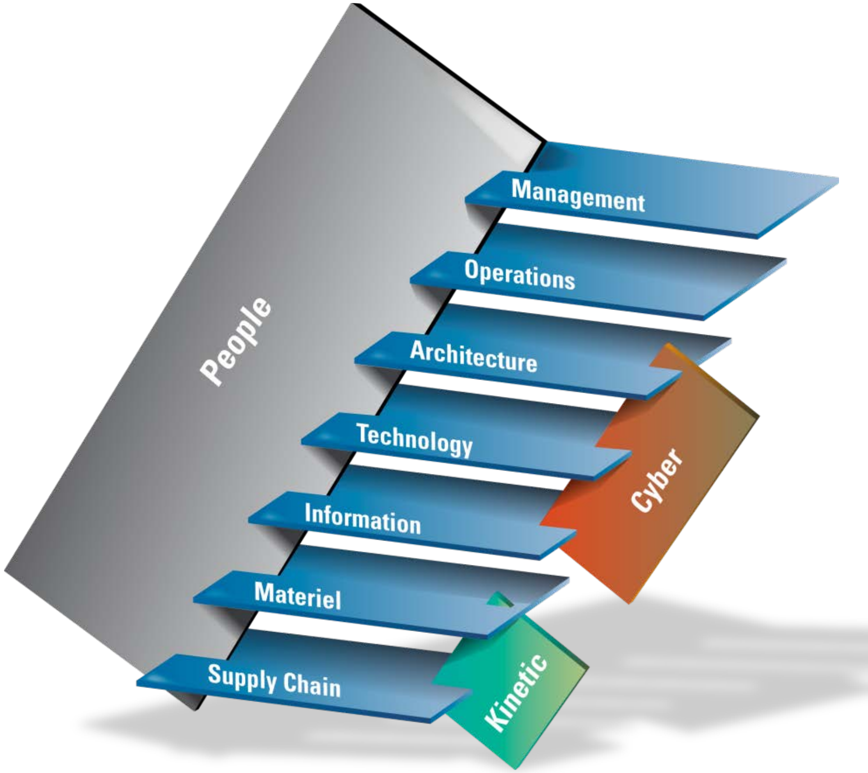
(Emergent properties don't emerge overnight)

Make a long-term commitment

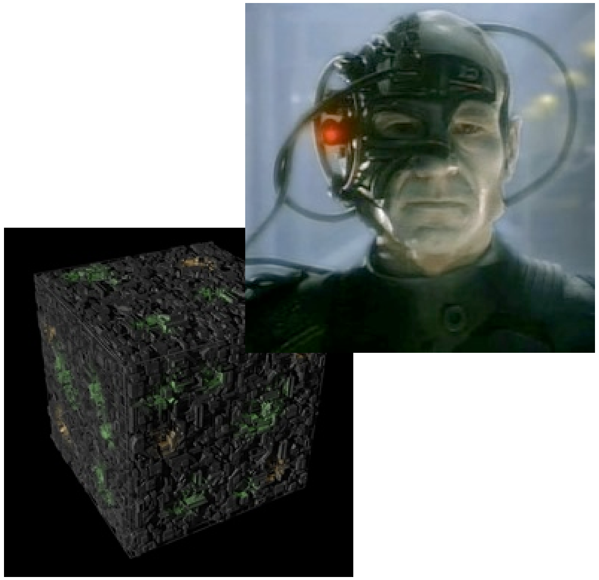
(It is not a sprint; it is a marathon)

Understand the big picture

(Organizations must address operational risk on a number of dimensions)

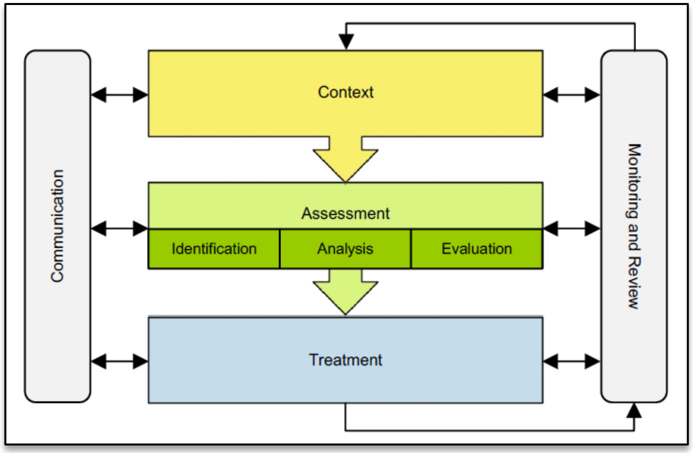


Prevention is futile



Cybersecurity is a risk management issue

(Not a technology issue)



Cybersecurity is a discussion topic for the Board

(Not for the data center)

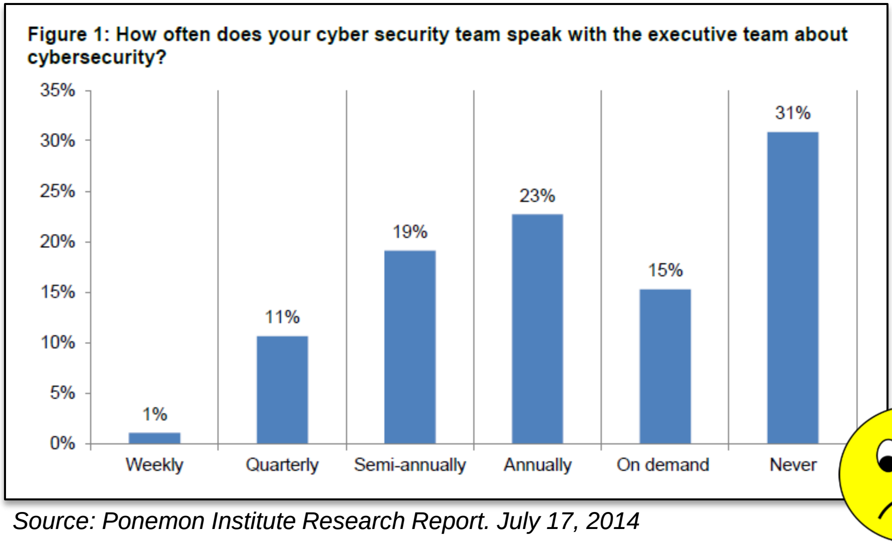
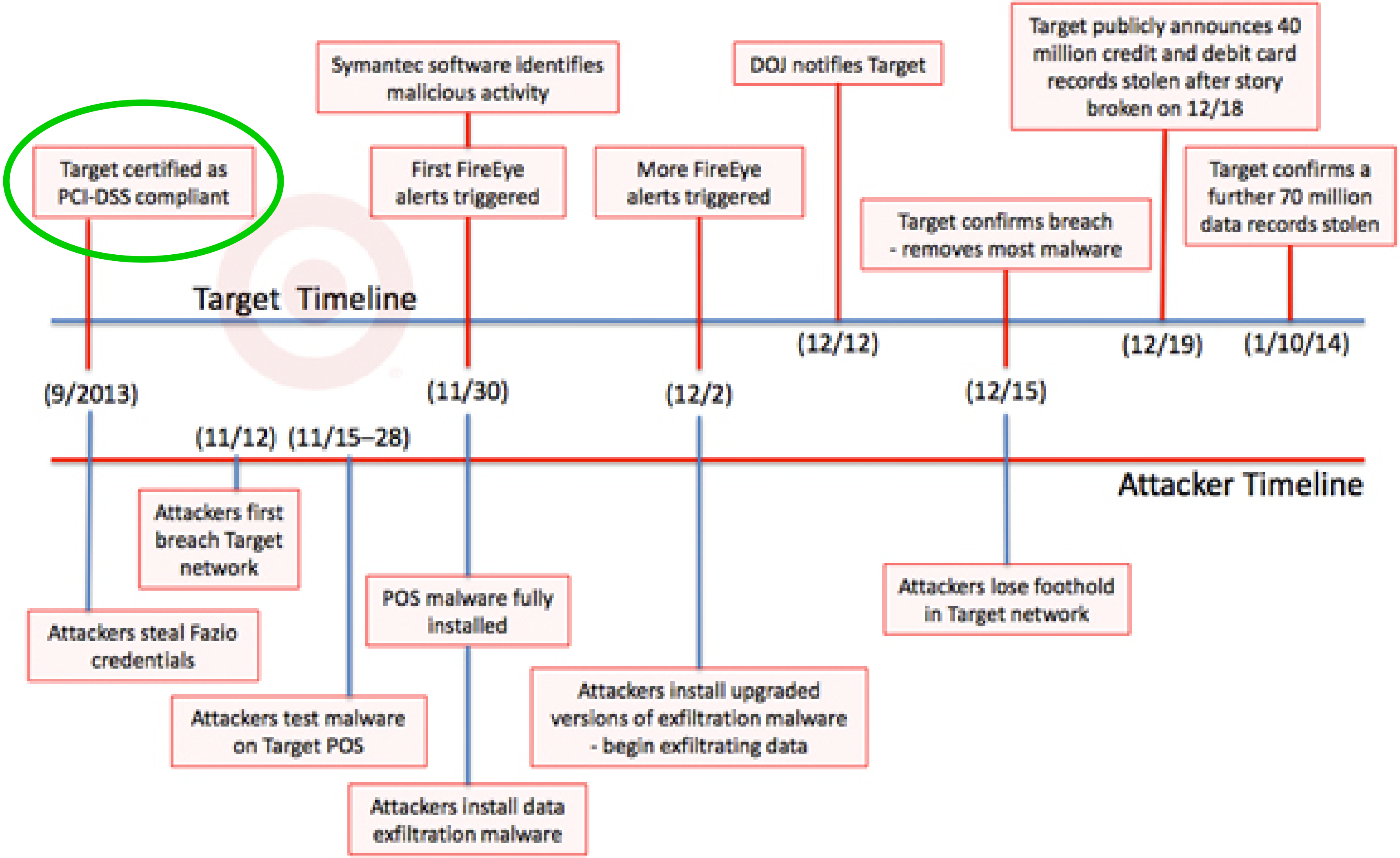


Figure 1: How often does your cyber security team speak with the executive team about cybersecurity?

Source: Ponemon Institute Research Report. July 17, 2014

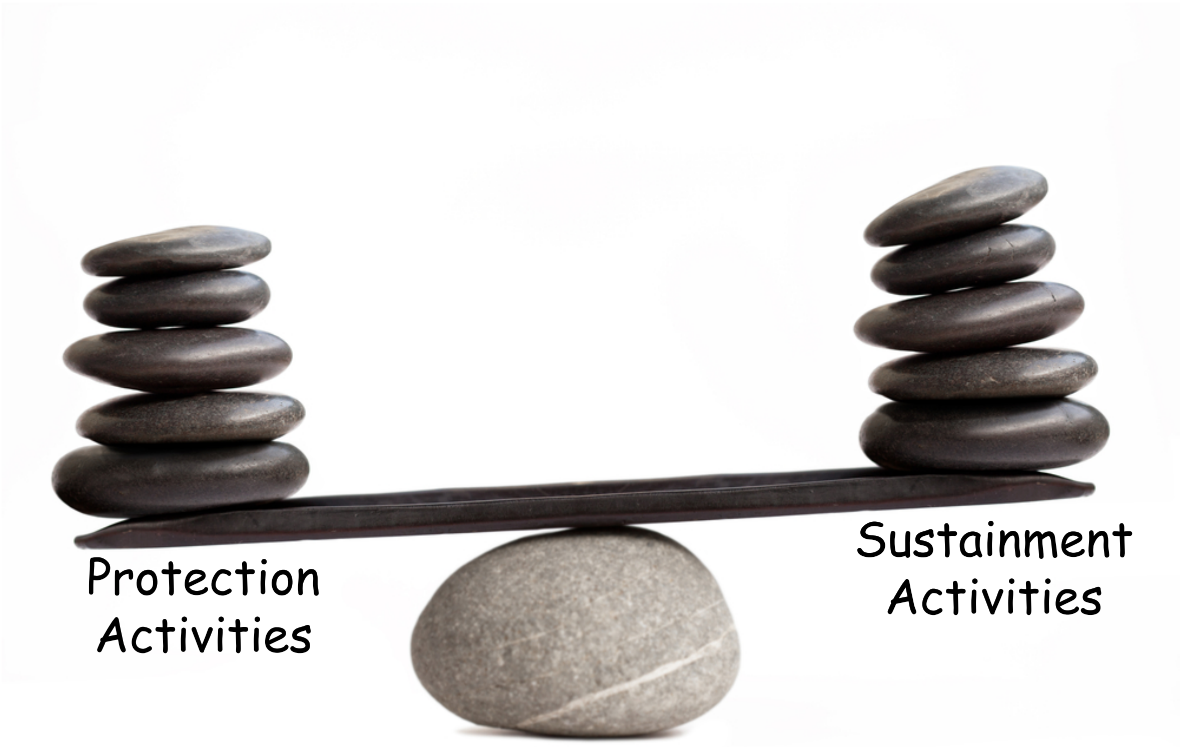
Compliance ≠ Security or Resilience

Timeline of the Target Data Breach

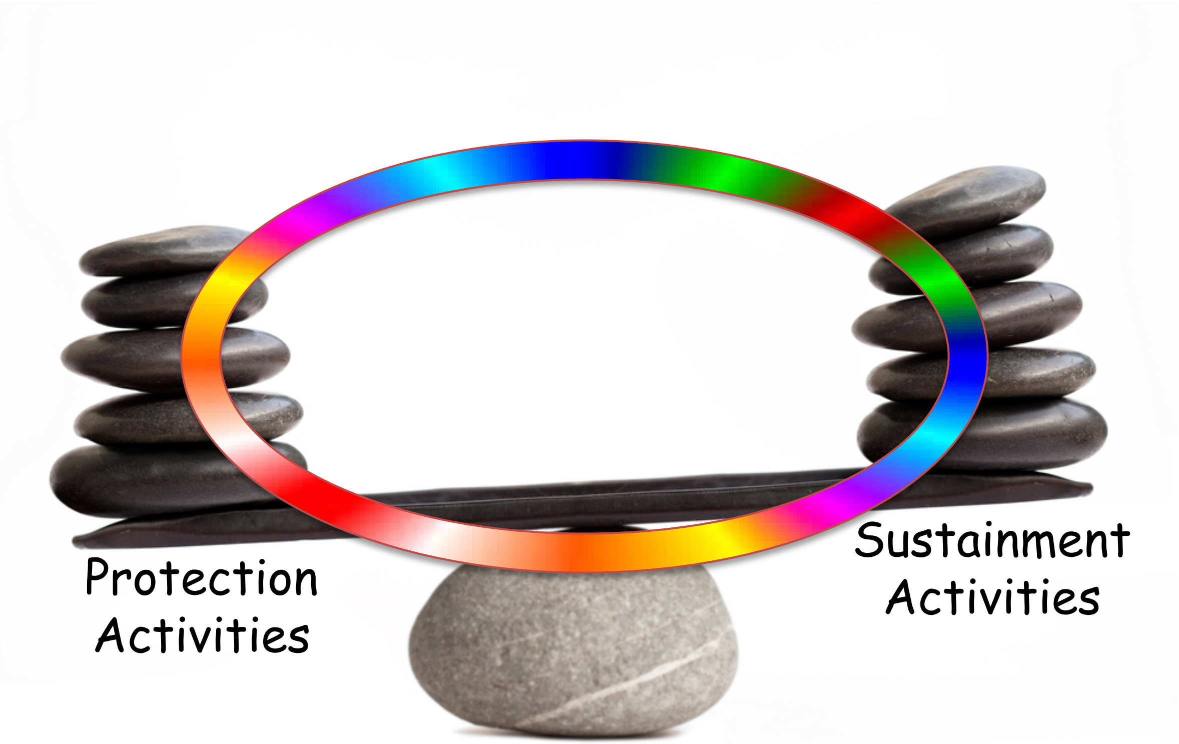

Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18
Symantec software identifies malicious activity
DOJ notifies Target
Target certified as PCI-DSS compliant
First FireEye alerts triggered
More FireEye alerts triggered
Target confirms breach - removes most malware
Target confirms a further 70 million data records stolen
Target Timeline
(12/12)
(12/19)
(1/10/14)
(9/2013)
(11/30)
(12/2)
(12/15)
(11/12)
(11/15–28)
Attacker Timeline
Attackers first breach Target network
POS malware fully installed
Attackers lose foothold in Target network
Attackers steal Fazio credentials
Attackers install upgraded versions of exfiltration malware - begin exfiltrating data
Attackers test malware on Target POS
Attackers install data exfiltration malware

Source: https://www.idradar.com/news-stories/identiy-protection/Target-Dropped-The-Ball-On-Breach-Detection-Report-Says

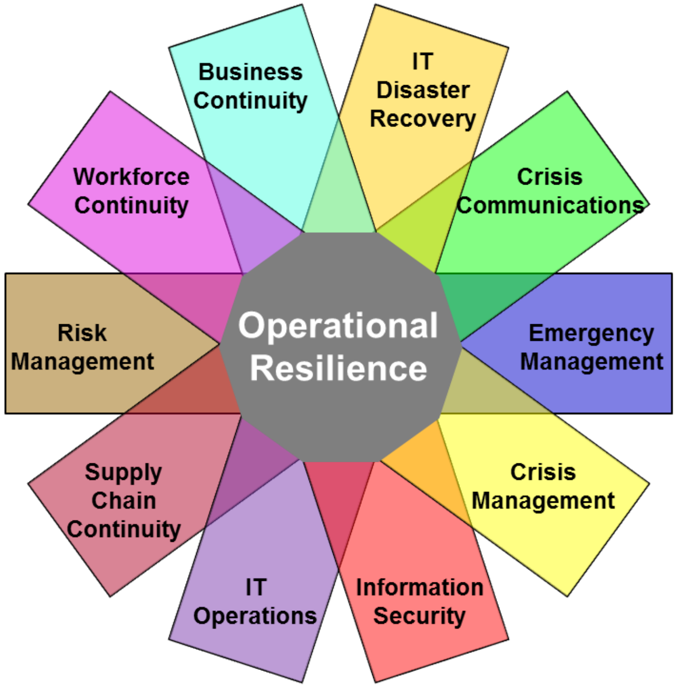
Continually balance protection and sustainment activities



Integrate and coordinate all operational risk management activities



Integrate and coordinate all operational risk management activities

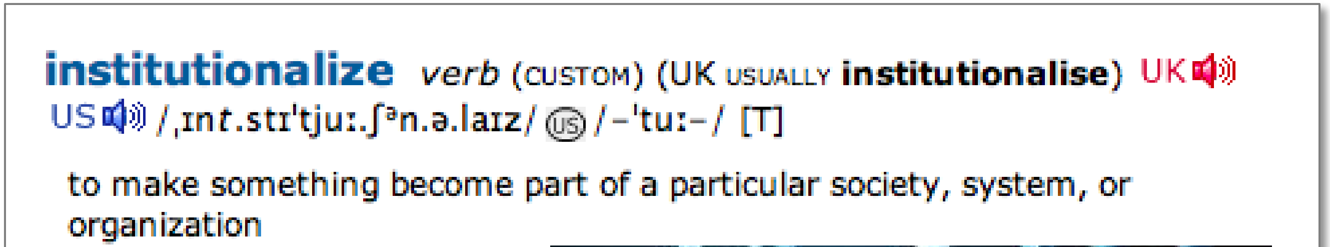


Invest in people and process

(Not only in technology)

Overcome organizational hurdles

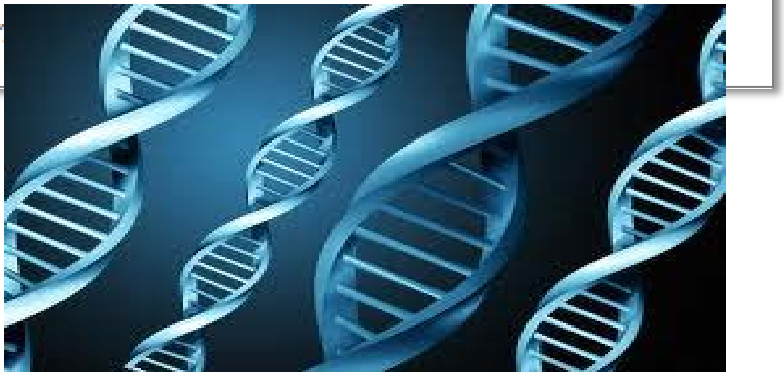
Create a culture of resilience



institutionalize *verb* (CUSTOM) (UK USUALLY **institutionalise**) UK US /ˌɪnt.stɪˈtjuː.ʃᵊn.ə.laɪz/ US /-ˈtuː-/ [T]

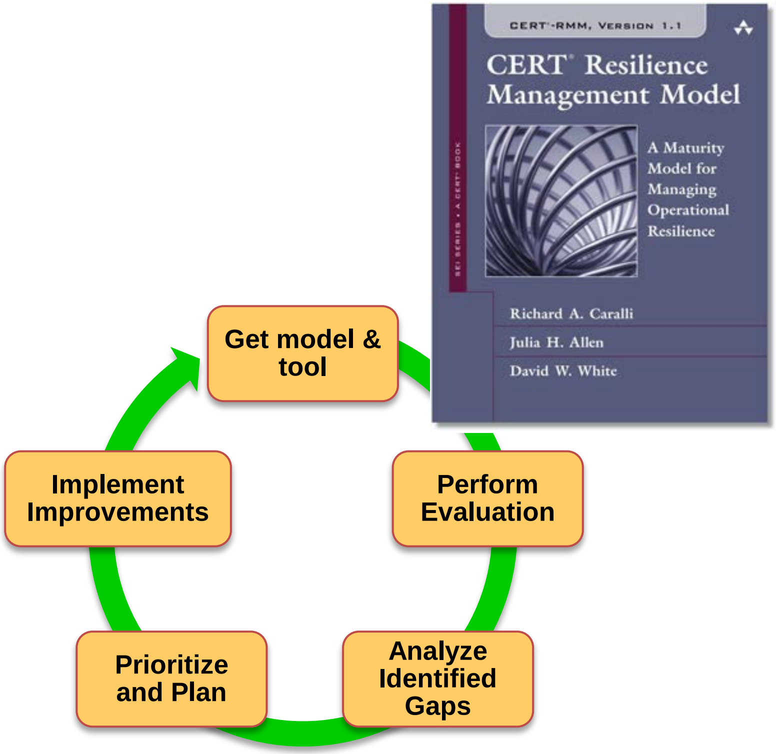
to make something become part of a particular society, system, or organization

What was once an inform



Establish governance (strategy, plan, sponsorship, performance) for operational resilience.

Utilize a proven and structured framework to guide resilience management activities



Get model & tool

Perform Evaluation

Analyze Identified Gaps

Prioritize and Plan

Implement Improvements

CERT-RMM, Version 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

Richard A. Caralli
Julia H. Allen
David W. White

“The oak fought the wind and was broken, the willow bent when it must and survived.”

Robert Jordan, The Fires of Heaven

Thank you for your attention…

Step-By-Step / Checklist / Roadmap …..

- ❑ Identify your critical products and services (Why do you exist?)
- ❑ What dose operational stress mean to you?
- ❑ Internal environmental scan (What has changed internally?)
- ❑ External environmental scan (What has changed externally?)
- ❑ Characterize your risk environment.
- ❑ What are your operational risks? Who will be affected if there are realized?
- ❑ What hurdles do you face to effective operational resilience management?
- ❑ What operational risk management activates (silos) exist? Are there opportunities for convergence of some sort?
- ❑ Draw the resilience context diagram for your organization.
- ❑ What are your resilience requirement categories?
- ❑ Repeat the exercise for your organization.
- ❑ Select an process improvement cycle? Do you already use one?
- ❑ Select a sample problem at your organization and do a model scoping exercise.

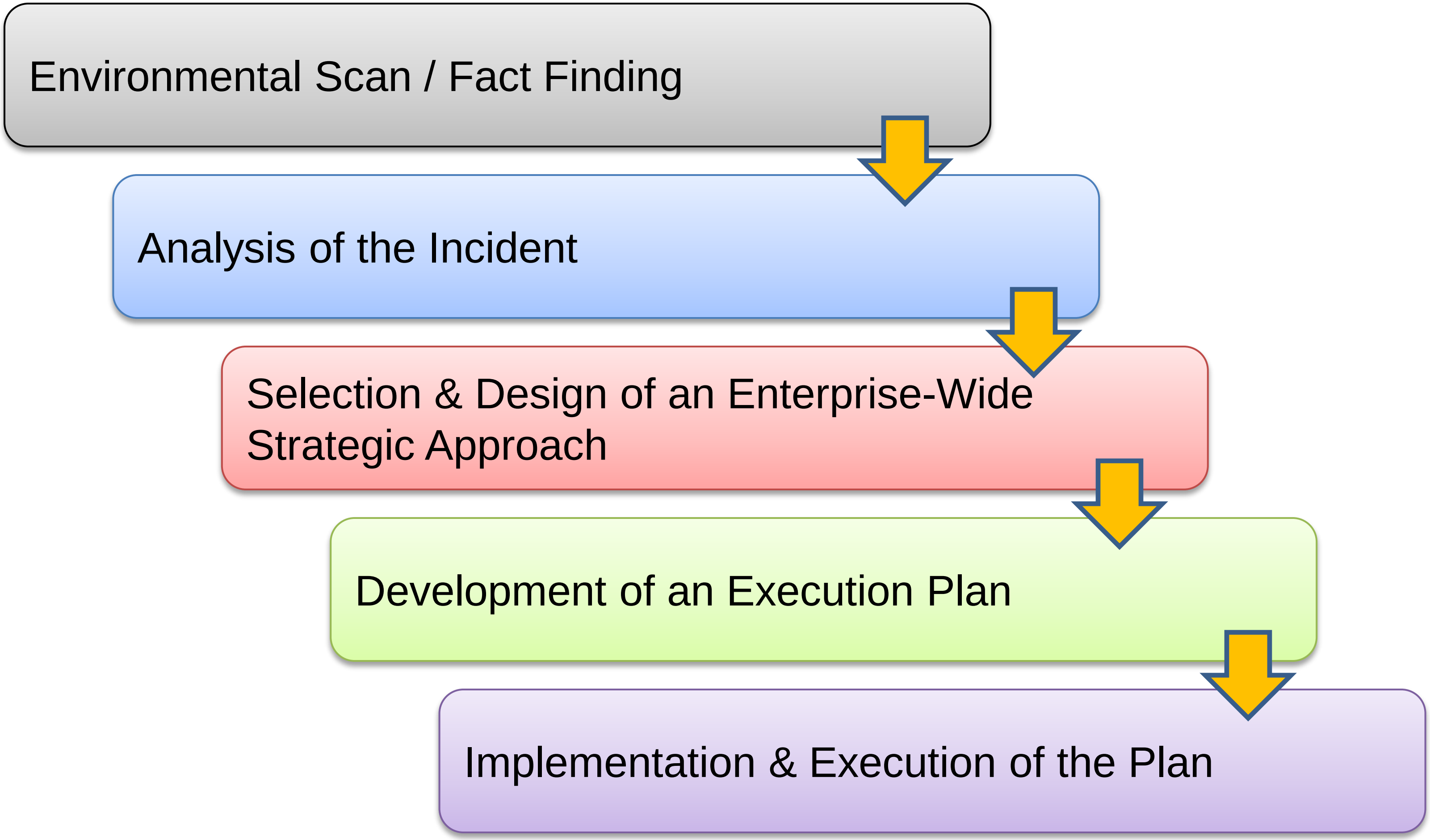
Guidance for Putting it into Practice

Two sample (very different) scenarios for putting principles of operational resilience into practice:

1. After a major and visible disruptive event has taken place and you want to apply concepts from his module to deal with it.

2. The there is a (business) desire to put in place a strategic plan and program to raise the bar.

Example 1a: After a Major Incident



Environmental Scan / Fact Finding

Analysis of the Incident

Selection & Design of an Enterprise-Wide Strategic Approach

Development of an Execution Plan

Implementation & Execution of the Plan

Example 1b: After a Major Incident

Environmental Scan / Fact Finding

- The Company
- The Incident

Analysis of the Incident

- Business Impact
- Root Causes
- Risk Assessment

Selection & Design of an Approach

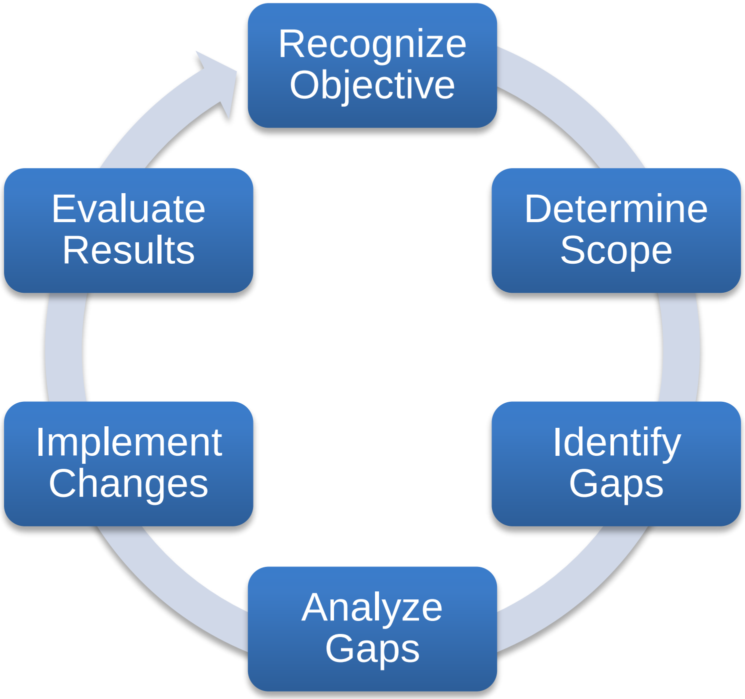
- Operational Resilience Management Approach
- Gap Analysis & Characterization of Current State
- Establishing Target State
- How to get there?

Development of an Execution Plan

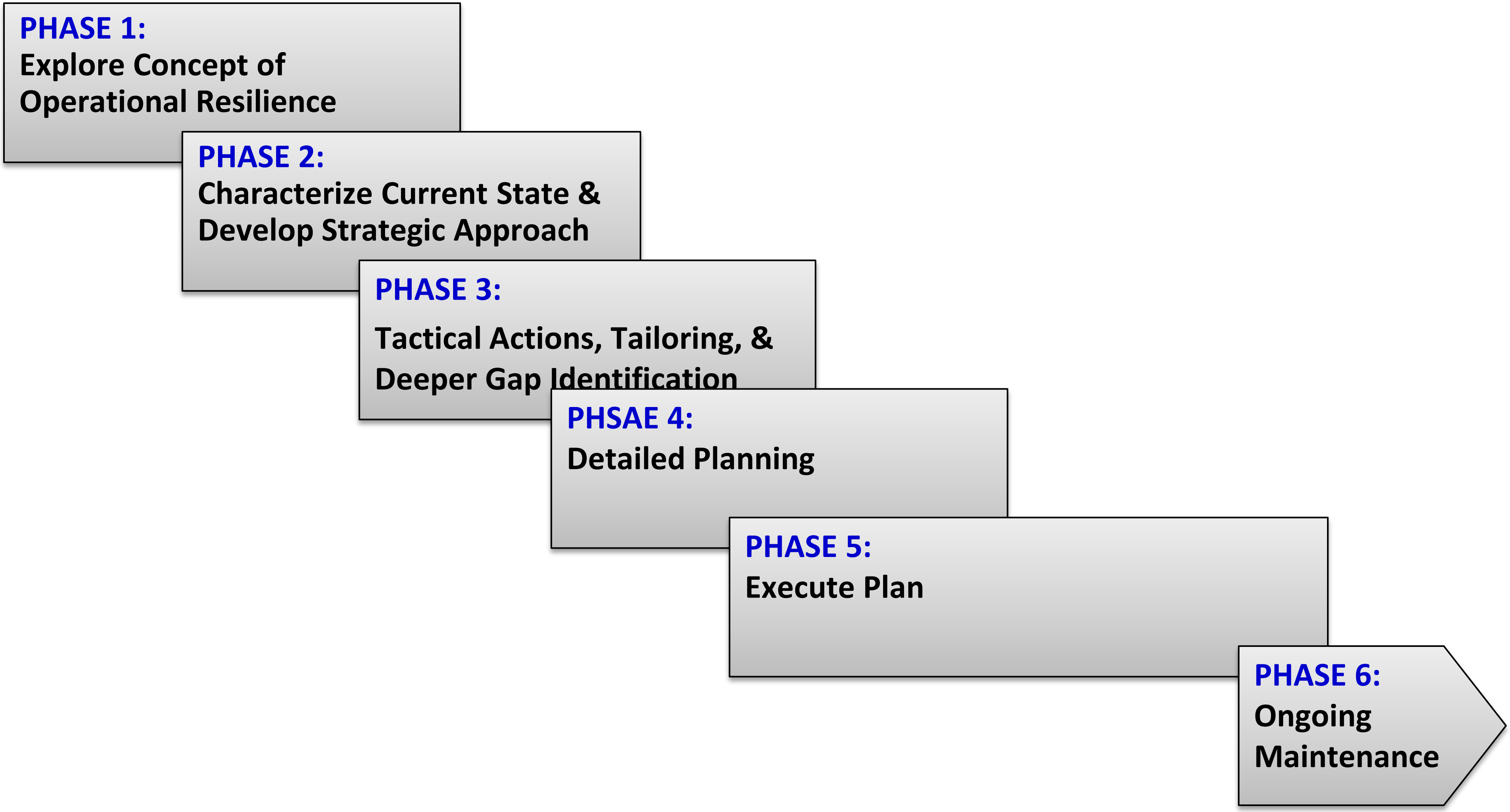
- Short-Term / Long-Term Corrective Actions
- Phase I, II, III, …

Implementation & Execution of the Plan

- Execution and Program Approach
- Roles and Responsibilities
- Timeline



Example 2a: Strategic Plan to Raise the Bar



PHASE 1:
Explore Concept of Operational Resilience

PHASE 2:
Characterize Current State & Develop Strategic Approach

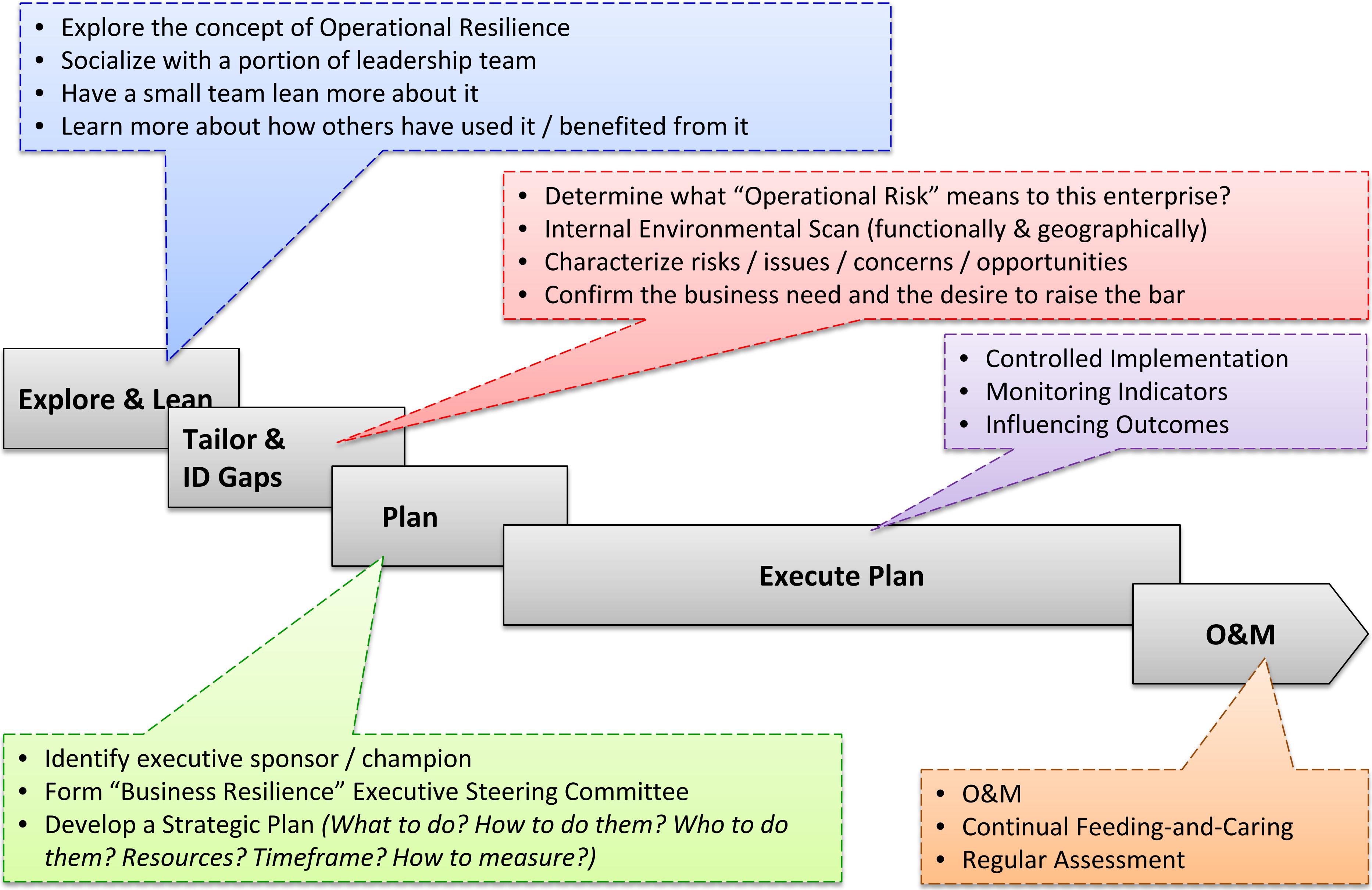
PHASE 3:
Tactical Actions, Tailoring, & Deeper Gap Identification

PHSAE 4:
Detailed Planning

PHASE 5:
Execute Plan

PHASE 6:
Ongoing Maintenance

Example 2b: Strategic Plan to Raise the Bar



Explore & Lean

- Explore the concept of Operational Resilience
- Socialize with a portion of leadership team
- Have a small team lean more about it
- Learn more about how others have used it / benefited from it

Tailor & ID Gaps

- Determine what “Operational Risk” means to this enterprise?
- Internal Environmental Scan (functionally & geographically)
- Characterize risks / issues / concerns / opportunities
- Confirm the business need and the desire to raise the bar

Plan

- Identify executive sponsor / champion
- Form “Business Resilience” Executive Steering Committee
- Develop a Strategic Plan *(What to do? How to do them? Who to do them? Resources? Timeframe? How to measure?)*

Execute Plan

- Controlled Implementation
- Monitoring Indicators
- Influencing Outcomes

O&M

- O&M
- Continual Feeding-and-Caring
- Regular Assessment